PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-293253
(43)Date of publication of application : 20.10.2000

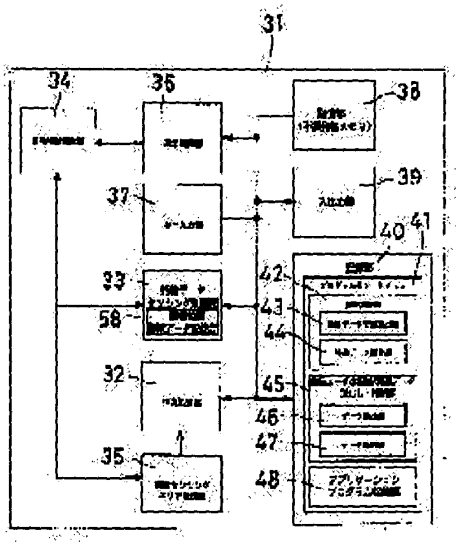
(51)Int.Cl. G06F 1/00

(21)Application number : 11-098138
(22)Date of filing : 05.04.1999

(71)Applicant : SHARP CORP
(72)Inventor : HIGAMI SADAHIKO
HARADA KOICHI

(54) INFORMATION PROCESSOR

(57)Abstract:
PROBLEM TO BE SOLVED: To provide an information processor provided with a fingerprint authenticating function having high security and excellent operability.
SOLUTION: When a fingerprint is inputted from the fingerprint reading face of a display/fingerprint reading part 34, a fingerprint data sensing control part 33 reads fingerprint data and coordinate data and stores them in a storage part 40. The fingerprint data is collated with fingerprint data previously registered and stored in a storage part 38. It is certified whether matched fingerprints exist or not. An information processor 31 realizes a fingerprint authenticating function in this way. The operation of the information processor 31 is controlled based on coordinate data related with fingerprint input. The operation of the information processor 31 can be controlled by a simple operation like the designation of a coordinate by the touch of a finger to the fingerprint reading face at the time of authenticating the fingerprint.



LEGAL STATUS

[Date of request for examination] 25.01.2002

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

* NOTICES *

1. This document has been translated by computer.So the translation may not reflect the original precisely.
2. **** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1] The information processor characterized by to be included a display means have the screen to which rectangular coordinates were set in an information processor equipped with a fingerprint authentication means collates the fingerprint read in the fingerprint reading side with the fingerprint memorized beforehand, and attest it, a coordinate specification means specify the coordinate relevant to the fingerprint read on the screen, and the control means that perform motion control based on the specified coordinate.
[Claim 2] The information processor according to claim 1 characterized by the aforementioned screen and a fingerprint reading side being the same.
[Claim 3] The information processor according to claim 1 characterized by forming the fingerprint reading side in the aforementioned coordinate specification means.
[Claim 4] The aforementioned control means are information processors according to claim 1 characterized by starting a fingerprint authentication means when a specific coordinate is specified.
[Claim 5] For the aforementioned control means, the aforementioned information processor is an information processor according to claim 1 characterized by performing motion control based on the authentication result of a personal identification number, including further a personal identification number acquisition means to acquire the personal identification number based on the specified coordinate, and a personal identification number authentication means to collate the acquired personal identification number with the personal identification number memorized beforehand, and to attest it.
[Claim 6] The aforementioned control means are information processors according to claim 5 characterized by starting a fingerprint authentication means when the personal identification number is in agreement.
[Claim 7] The aforementioned control means are information processors according to claim 1 characterized by controlling operation of the power supply of an information processor when the fingerprint is in agreement.
[Claim 8] The aforementioned control means are information processors according to claim 1 characterized by reading and setting up the operating condition corresponding to the user of the fingerprint which was in agreement out of the operating condition beforehand set up for every user when the fingerprint was in agreement.
[Claim 9] The aforementioned fingerprint authentication means is an information processor according to claim 1 characterized by fingerprint authentication of each finger being possible.
[Claim 10] The aforementioned control means are information processors according to claim 9 characterized by reading and executing the command corresponding to each finger of the user of the fingerprint which was in agreement out of the command beforehand registered for every finger of a user when the fingerprint of each finger was in agreement.
[Claim 11] An icon setting means to set up the icon corresponding to application in the aforementioned information processor, An icon specification judging means to judge whether the icon set up based on the specified coordinate was specified is included further. the aforementioned control means The information processor according to claim 1 characterized by reading and displaying only the data of the user of a fingerprint with whom the application corresponding to the specified icon was in agreement when an icon is specified and a fingerprint is in agreement.
[Claim 12] The aforementioned control means are information processors according to claim 11 characterized by starting the application corresponding to the user of a fingerprint with whom it was [in the application beforehand set up for every user] in agreement when an icon is specified and a fingerprint is in agreement.
[Claim 13] The aforementioned control means are information processors according to claim 11 characterized by opening only the file of the user of a fingerprint which corresponded when the file for every user is matched with the aforementioned icon, and an icon is specified and a fingerprint is in agreement.
[Claim 14] A menu runlevel field setting means to set up the field corresponding to the runlevel of a menu in the aforementioned information processor, A menu runlevel block-definition judging means to judge whether the menu runlevel field set up based on the specified coordinate was specified is included further. the aforementioned control means When a menu runlevel field is specified and a fingerprint is in agreement, by the runlevel of the menu runlevel field which is a runlevel corresponding to the user of a fingerprint with whom it was [in the runlevel beforehand set up for every user] in agreement, and was specified The information processor according to claim 1 characterized by performing a menu.
[Claim 15] It is the information processor according to claim 1 which the documents which have the seal column are displayed on the aforementioned display means, the aforementioned control means add the recognition mark to the seal column of the aforementioned documents when the detected coordinate is a coordinate of the seal column, and the aforementioned information processor carries out [that the means of communications for communicating the documents with which the recognition mark was added further is included, and] as the feature.
[Claim 16] It is the information processor according to claim 1 the documents which have the seal column are displayed on the aforementioned display means, the aforementioned control means add the recognition mark to the seal column of the aforementioned

documents when the detected coordinate is a coordinate of the seal column, and the aforementioned information processor carries out containing an incidental processing means carry out incidental processing to the documents with which the recognition mark was added further as the feature.

[Translation done.]

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[The technical field to which invention belongs] this invention relates to an information processor equipped with a fingerprint authentication function.
[0002]
[Description of the Prior Art] By development of network society, fusion to an information processor and a network progresses and the need for security functions, such as individual authentication, has been increasing. As individual authentication, an information processor is hard to be abused for others, and authentication by biological information which does not have the possibility of loss like a key or IC (integrated circuit) card, such as a fingerprint, attracts attention. Although the thing using optical system, such as prism, as a reading method of a fingerprint is in use, for example, is indicated by JP,8-315143,A, the technology which adjoins the TFT (TFT) element of a liquid crystal display, arranges a photodiode, carries out like CCD (charge-coupled device), and reads a picture is indicated by JP,9-186312,A. Moreover, the technology about the technique of fingerprint discernment is indicated by JP,7-220075,A and JP,10-154231,A. Furthermore, the technology about the motion control of an information processor based on a fingerprint authentication result is indicated by JP,10-69324,A.
[0003] Drawing 24 is the block diagram of the information processor 1 of the conventional technology equipped with a fingerprint authentication function. Moreover, drawing 25 is drawing showing the fingerprint read station 4 and display 7 of an information processor 1. The I/O section 9 and the storage section 10 for connection with peripheral devices, such as connection with the display-control section 6 which controls the displays 7, such as the key input sections 5, such as the fingerprint data sensing control section 3 which controls the fingerprint read station 4, and a keyboard, and a liquid crystal display, the storage section 8 realized by non-volatile memory, and a network, and a printer, are connected to the central-process section 2 of an information processor 1, and operation of the whole equipment is controlled in generalization.
[0004] A user's registration data are memorized by the storage section 8, and it is read by the central-process section 2 if needed, and it is transmitted to the storage section 10 and stored in it. In addition, an application program is similarly memorized by the storage section 8, and the central-process section 2 reads it if needed, and although it transmits to the storage section 10 and is stored in it, you may memorize in the storage section 10.
[0005] The fingerprint read station 4 is realized by the method of JP,8-315143,A and the technology of JP,9-186312,A using optical system which was mentioned above. After the fingerprint read by the fingerprint read station 4 is stored temporarily in the fingerprint data-storage section 21 of the fingerprint data sensing control section 3, it is given to the storage section 10.
[0006] The storage section 10 is equipped with the program work memory 11 which consists of fingerprint read-out, the storing sections 15, and the application program storing sections 18 of the registration user who has the fingerprint authentication section 12 and the data read-out section 16 which have the feature-extraction section 13 of fingerprint data, and the collating section 14 of the feature data, and the data storage section 17.
[0007] In the information processor 1 of the conventional technology, as shown in drawing 25 (A), the screen 19 of the fingerprint read station 4 and a display 7 is formed independently. moreover -- or as shown in drawing 25 (B), the fingerprint reading side 20 of the fingerprint read station 4 and the screen 19 of a display 7 are formed independently For this reason, motion control of the information processor 1 using the coordinate about fingerprint read is not performed.
[0008]
[Problem(s) to be Solved by the Invention] The purpose of this invention is offering an information processor equipped with the fingerprint authentication function having high security nature and high operability.
[0009]
[Means for Solving the Problem] this invention is the information processor characterized by to be included a display means have the screen to which rectangular coordinates were set, a coordinate specification means specify the coordinate relevant to the fingerprint read on the screen, and the control means that perform motion control based on the specified coordinate in an information processor equipped with a fingerprint authentication means collates the fingerprint read in the fingerprint reading side with the fingerprint memorized beforehand, and attest it.
[0010] If this invention is followed, the fingerprint read in the fingerprint reading side will be collated with the fingerprint memorized beforehand, and authentication of whether there is any fingerprint in agreement will be made. In an information processor, it does in this way and a fingerprint authentication function is realized. Moreover, at the time of fingerprint authentication, the coordinate relevant to the fingerprint read on the screen of a display means is specified by the coordinate specification means. Control means control operation of an information processor based on the specified coordinate. Thus, operation of an information processor is controllable by the easy operation of the coordinate specification at the time of fingerprint authentication.
[0011] Moreover, this invention is characterized by the aforementioned screen and a fingerprint reading side being the same. If this

invention is followed, at the time of fingerprint authentication, a user's finger will be contacted by the screen which is a fingerprint reading side, and the fingerprint which did in this way and was read in the fingerprint reading side will be collated and attested. Moreover, the coordinate relevant to the fingerprint read on the screen, i.e., the coordinate of the position which contacted the finger, is specified at the time of contact of a finger. Control means control operation of an information processor based on the coordinate specified by such easy operation. Since the screen and a fingerprint reading side are the same, fingerprint input and coordinate specification can be performed by the same operation, and high operability is acquired.

[0012] Moreover, this invention is characterized by forming the fingerprint reading side in the aforementioned coordinate specification means.

[0013] If this invention is followed, at the time of fingerprint authentication, a user's finger will be contacted in the fingerprint reading side formed in the coordinate specification means, and the fingerprint which did in this way and was read in the fingerprint reading side will be collated and attested. Moreover, the coordinate relevant to the fingerprint read on the screen is specified by the coordinate specification means. Control means control operation of an information processor based on the coordinate specified by such easy operation. Since a fingerprint reading side is formed in a coordinate specification means, coordinate specification and a fingerprint input can be performed by the same operation, and high operability is acquired.

[0014] Moreover, the aforementioned control means are characterized by starting a fingerprint authentication means, when, as for this invention, a specific coordinate is specified.

[0015] When following this invention and the specified coordinate is a specific coordinate, operation of an information processor can be controlled to start a fingerprint authentication means. Therefore, when coordinates other than a specific coordinate are specified, as fingerprint authentication is not performed, high security nature can be obtained.

[0016] Moreover, this invention is characterized by the aforementioned control means performing motion control based on the authentication result of a personal identification number, including further a personal identification number acquisition means to acquire the personal identification number based on the coordinate the aforementioned information processor was specified to be, and a personal identification number authentication means to collate the acquired personal identification number with the personal identification number memorized beforehand, and to attest it.

[0017] If this invention is followed, as the fingerprint authentication function was mentioned above, it will be realized. Moreover, the coordinate relevant to the fingerprint read on the screen of a display means is specified by the coordinate specification means, and the personal identification number based on the specified coordinate is acquired by the personal identification number acquisition means. The acquired personal identification number is collated with the personal identification number memorized beforehand, and authentication in agreement is made. In an information processor, it does in this way again and the authentication function of a personal identification number is realized. Control means control operation of an information processor based on the authentication result of a personal identification number. Thus, operation of an information processor is controllable by the easy operation of the coordinate specification for inputting the personal identification number at the time of fingerprint authentication.

[0018] Moreover, this invention is characterized by starting a fingerprint authentication means, when the aforementioned control means of a personal identification number correspond.

[0019] When following this invention and the acquired personal identification number is in agreement with the personal identification number memorized beforehand, operation of an information processor can be controlled to start a fingerprint authentication means. Therefore, when numbers other than a specific personal identification number are acquired, as fingerprint authentication is not performed, high security nature can be obtained.

[0020] Moreover, this invention is characterized by controlling operation of the power supply of an information processor, when the aforementioned control means of a fingerprint correspond.

[0021] When following this invention and it is in agreement with the fingerprint with which the read fingerprint was beforehand memorized as a result of the performed fingerprint authentication, ON/OFF operation of the power supply of an information processor is controlled. For example, when the fingerprint is in agreement, a power supply is made into an ON state from an OFF state. Thus, high security nature and high operability can be acquired, and reduction of power consumption can be aimed at.

[0022] Moreover, this invention is characterized by the aforementioned control means reading and setting up the operating condition corresponding to the user of the fingerprint which was in agreement out of the operating condition beforehand set up for every user when the fingerprint was in agreement.

[0023] When following this invention and it is in agreement with the fingerprint with which the read fingerprint was beforehand memorized as a result of the performed fingerprint authentication, the operating condition corresponding to the user of the fingerprint which was in agreement out of the operating condition beforehand set up for every user is read and set up. Therefore, the operating environment and the use function to have been suitable for the user can be set up, and high operability is acquired.

[0024] Moreover, as for the aforementioned fingerprint authentication means, this invention is characterized by fingerprint authentication of each finger being possible.

[0025] If this invention is followed, since fingerprint authentication of each finger is possible in the aforementioned fingerprint authentication function, the fine motion control of an information processor based on the fingerprint authentication result of each finger becomes possible.

[0026] Moreover, this invention is characterized by the aforementioned control means reading and executing the command corresponding to each finger of the user of the fingerprint which was in agreement out of the command beforehand registered for every finger of a user when the fingerprint of each finger was in agreement.

[0027] When following this invention and it is in agreement with the fingerprint of each finger with which the fingerprint of each finger was memorized beforehand in the aforementioned fingerprint authentication function in which fingerprint authentication of each finger is possible, the command corresponding to each finger of the user of the fingerprint which was in agreement out of the command beforehand registered for every finger of a user is read and executed. Thus, high security nature and high operability can be acquired, and the fine motion control for every finger becomes possible.

[0028] Moreover, an icon setting means to set up the icon corresponding to [this invention] application in the aforementioned information processor, An icon specification judging means to judge whether the icon set up based on the specified coordinate was specified is included further. the aforementioned control means When an icon is specified and a fingerprint is in agreement, it is characterized by reading and displaying only the data of the user of a fingerprint with whom the application corresponding to the specified icon was in agreement.

[0029] If this invention is followed, as the fingerprint authentication function was mentioned above, it will be realized. Moreover, the coordinate relevant to the fingerprint read on the screen of a display means is specified by the coordinate specification means. An icon specification judging means judges whether based on the specified coordinate, the icon set up by the icon setting means was specified. Control means control operation of an information processor based on this judgment result and a fingerprint authentication result. That is, when an icon is specified and a fingerprint is in agreement, only the data of the user of a fingerprint with whom the application corresponding to the specified icon was in agreement are read and displayed. Thus, operation of an information processor is controllable by the easy operation of the coordinate specification at the time of fingerprint authentication.

[0030] Moreover, it is characterized by starting the application corresponding to the user of a fingerprint with whom it was [in the application with which this invention was beforehand set up for every user when an icon was specified and the aforementioned control means of a fingerprint corresponded] in agreement.

[0031] If this invention is followed, control means will control operation of an information processor based on the judgment result and fingerprint authentication result of icon specification. That is, when an icon is specified and a fingerprint is in agreement, the application corresponding to the user of a fingerprint with whom it was [in the application beforehand set up for every user] in agreement is started. Thus, operation of an information processor is controllable by the easy operation of the coordinate specification at the time of fingerprint authentication.

[0032] Moreover, the aforementioned control means are characterized by opening only the file of the user of a fingerprint which corresponded, when, as for this invention, the file for every user is matched with the aforementioned icon, and an icon is specified and a fingerprint is in agreement.

[0033] If this invention is followed, control means will control operation of an information processor based on the judgment result and fingerprint authentication result of icon specification. That is, when an icon is specified and a fingerprint is in agreement, only the file of the user of a fingerprint which corresponded is opened. Thus, operation of an information processor is controllable by the easy operation of the coordinate specification at the time of fingerprint authentication.

[0034] Moreover, a menu runlevel field setting means to set up the field corresponding to [this invention] the runlevel of a menu in the aforementioned information processor, A menu runlevel block-definition judging means to judge whether the menu runlevel field set up based on the specified coordinate was specified is included further. the aforementioned control means When a menu runlevel field is specified and a fingerprint is in agreement, it is a runlevel corresponding to the user of a fingerprint with whom it was [in the runlevel beforehand set up for every user] in agreement, and is characterized by performing a menu by the runlevel of the specified menu runlevel field.

[0035] If this invention is followed, as the fingerprint authentication function was mentioned above, it will be realized. Moreover, the coordinate relevant to the fingerprint read on the screen of a display means is specified by the coordinate specification means. A menu runlevel block-definition judging means judges whether based on the specified coordinate, the menu runlevel field set up by the menu runlevel field setting means was specified. Control means control operation of an information processor based on this judgment result and a fingerprint authentication result. That is, when a menu runlevel field is specified and a fingerprint is in agreement, it is a runlevel corresponding to the user of a fingerprint with whom it was [in the runlevel beforehand set up for every user] in agreement, and a menu is performed by the runlevel of the specified menu runlevel field. Thus, operation of an information processor is controllable by the easy operation of the coordinate specification at the time of fingerprint authentication.

[0036] Moreover, the documents with which this invention has the seal column for the aforementioned display means are displayed, the aforementioned control means add the recognition mark to the seal column of the aforementioned documents, when the detected coordinate is a coordinate of the seal column, and it carries out that the aforementioned information processor contains further the means of communications for communicating the documents with which the recognition mark was added as the feature.

[0037] The recognition mark is added, when following this invention and the coordinate specified in relation to fingerprint read to the documents which have the seal column is a coordinate in the seal column. Furthermore, the documents with which the recognition mark was added communicate by means of communications. Therefore, documents, such as a report, can be transmitted and circulated to the next man.

[0038] Moreover, the documents with which this invention has the seal column for the aforementioned display means are displayed, the aforementioned control means add the recognition mark to the seal column of the aforementioned documents, when the detected coordinate is a coordinate of the seal column, and it carries out containing an incidental processing means carry out incidental processing to the documents with which, as for the aforementioned information processor, the recognition mark was added further as the feature.

[0039] The recognition mark is added, when following this invention and the coordinate specified in relation to fingerprint read to the documents which have the seal column is a coordinate in the aforementioned seal column. Furthermore, the incidental means of the documents with which the recognition mark was added is carried out by the incidental processing means. Therefore, issue processing of an order sheet can be performed to documents, such as settlement-of-accounts ******.

[0040]

[Embodiments of the Invention] Drawing 1 is the block diagram of the information processor 31 which is one form of operation of this invention. In the central-process section 32 of the information processor 31 equipped with a fingerprint authentication function Fingerprint reading operation of a display and the fingerprint read station 34 The fingerprint data sensing control section 33 to control, The I/O section 39 for connection with peripheral devices, such as connection with the key input sections 37, such as the display-control section 36 which controls the display action of the fingerprint sensing area setting section 35, and the display and a fingerprint

read station 34, and a keyboard, the storage section 38 realized by non-volatile memory, and a network, and a printer And the storage section 40 is connected and operation of the whole equipment is controlled in generalization.

[0041] The screen to which the rectangular coordinates of the display realized with a liquid crystal display were set, and the fingerprint reading side where the finger of the fingerprint read station realized by well-known technology is contacted are [in / a display and the fingerprint read station 34] the same. Specifically, the sensor for data read is formed in all the pixels of a liquid crystal display. It is necessary to form this sensor in no pixels of a liquid crystal display, and it may be formed only in some pixels. Thus, the coordinate data and fingerprint data on Screen 59 are acquired by the display and the fingerprint read station 34 which has the display and the data reading screen 59 shown in drawing 2 . The central-process section 32 controls operation of an information processor 31 based on the acquired coordinate data, and controls operation of equipment 31 based on the acquired fingerprint data.

[0042] In addition, it is the picture reader indicated to Japanese Patent Application No. No. 12231 [11 to] by the applicant for this patent as a display and a fingerprint read station 34, and the picture reader which embeds a photo detector to the interior of a liquid crystal layer, and reads fingerprint data may be adopted. In an information processor 31, a fingerprint reading means, a display means, and a coordinate specification means are realized by a display and the fingerprint read station 34.

[0043] In the coordinate position and the fingerprint data-storage section 58 of the fingerprint data sensing control section 33, the coordinate data and fingerprint data which were acquired by the display and the fingerprint read station 34 are stored temporarily. These stored data are transmitted to the storage section 40. An indicative data is given to a display and the fingerprint read station 34 from the display-control section 36. Moreover, control of the timing of the display action of a display and the fingerprint read station 34 and fingerprint reading operation is performed by the central-process section 32.

[0044] The fingerprint sensing area setting section 35 sets up the fingerprint reading field 60 all over Screen 59. This field 60 is a rectangle field which makes the coordinate of two points specified by directions meanses, such as for example, an input pen, the peak which faced each other. From the key input section 37, the addition data to fingerprint data etc. are inputted if needed.

[0045] The user registration data registered beforehand are memorized by the storage section 38, and it is read by the central-process section 32 if needed, and it is transmitted to the storage section 40 and stored in it. In addition, an application program is similarly memorized by the storage section 38, and the central-process section 32 reads it if needed, and although it transmits to the storage section 40 and is stored in it, you may memorize in the storage section 40.

[0046] The storage section 40 is equipped with the program work memory 41 which consists of the fingerprint authentication section 42, read-out and the storing section 45 of a user's registration data, and the application program storing section 48. The fingerprint authentication section 42 has the feature-extraction section 43 which extracts the feature data of fingerprint data, and the collating section 44 which collates the extracted feature data. Read-out and the storing section 45 of a user's registration data have the data read-out section 46 which reads user registration data, and the data storage section 47 which stores the read user registration data.

[0047] Drawing 3 is drawing showing the user registration data of the storage section 38. User registration data consist of the master data sections 61 and the related data divisions 62 for every user. The master data section 61 consists of a user's name data storage section 63, the storing section 64 of fingerprint data, and the storing section 65 of an executive and substitute settlement-of-accounts person data. Fingerprint data 64a of left-hand each finger and fingerprint data 64b of right-hand each finger are stored in the storing section 64 of the aforementioned fingerprint data, respectively. The related data division 62 consist of the storing section 66 of operating environment data, the storing section 67 of the limit data of a use function, the storing section 68 of the shortcut data of each finger, the storing section 69 of authority data, and the storing section 70 of the setting data of starting application. Device setting change level 69a, network connection change level 69b, and other data 69c are stored in the storing section 69 of the aforementioned authority data, respectively.

[0048] An operating environment is data which specify the graphic size as which it is turned on/turned off and specific keys, such as a display/non-display one of specific information, such as help information which is equivalent to the operating condition of an information processor 31, for example, performs operation guidance, and a screen key, are displayed. It is data which specify good/improper one of data read-out from CD(compact disk)-ROM (read-only memory) which the limit data of a use function are also equivalent to an operating condition, for example, is connected, good/failure of use of SIO (file transfer protocol), etc. The shortcut data of each finger are a command which is equivalent to the command beforehand set up for every finger of a user, for example, specifies execution of the add function of a schedule. Authority data are data which specify device setting change level, network connection change level, etc. Starting application is the application of the network connection performed when sealed by the application and the report of order sheet issue which are performed when sealed by settlement-of-accounts ******.

[0049] Drawing 4 is a flow chart which shows the 1st operation of an information processor 31. At Step a1, the element 32 required for the read of a fingerprint, i.e., the central-process section, the fingerprint data sensing control section 33, and a display and a fingerprint read station 34 are made into a power supply ON state, and the element which is not required for the read of a fingerprint waits for a fingerprint input the detection period of a comparatively late fingerprint input as a power supply OFF state. This state is maintained until there is an input of a fingerprint, and it does in this way, and reduction of power consumption is achieved.

[0050] At the following step a2, the central-process section 32 judges whether there was any operation of the power supply ON by contact of the finger to a display and the data reading screen 59 of a display and the fingerprint read station 34. A finger is contacted, and if it judges that there was power supply ON operation, it will progress to the following step a3. If a finger is contacted, the fingerprint data sensing control section 33 will generate an interrupt signal to the central-process section 32. Based on this interrupt signal, the central-process section 32 makes a judgment with operation of power supply ON. moreover -- or the central-process section 32 makes a judgment with operation of power supply ON by read-out of the status by the polling from the central-process section 32 to the fingerprint data sensing processing section 33

[0051] At Step a3, the power supply state of the information-processor 31 whole is set to ON, and the fingerprint data sensing control section 33 reads the coordinate data of the position where fingerprint data and the finger were contacted from a display and the fingerprint read station 34, and stores it temporarily in the storage section 58. These data are transmitted to the storage section 40 through the central-process section 32. moreover -- or it is transmitted as it is to the storage section 40 by DMA (direct memory

access), without minding the central-process section 32
[0052] At the following step a4, the central-process section 32 judges whether the position by the acquired coordinate data is a specific position. When it is a specific position, it progresses to Step a5, and when it is not a specific position, it returns to Step a2.
[0053] At Step a5, the central-process section 32 reads the fingerprint data of the user registration data registered into the storage section 38, and stores them in the storage section 40. At the following step a6, the central-process section 32 collates and attests the acquired fingerprint data and the fingerprint data read from the storage section 38 by the fingerprint authentication program memorized by the storage section 40. At the following step a7, it judges whether the fingerprint is in agreement. When in agreement, a power supply ON state is maintained and operation is ended. When not in agreement, it progresses to Step a8.
[0054] At Step a8, it judges whether there are still any fingerprint data registered into the storage section 38, and fingerprint authentication operation is repeated until the fingerprint data still registered into Step a5 by returning at a certain time are lost. When there are already no fingerprint data registered, it progresses to Step a9, and an error message is performed, and it returns to Step a1.
[0055] In addition, the fingerprint authentication program memorized by the storage section 40 is read from the storage section 38, and is stored. This program may repeat and use the program which did not need to read and store in the degree of fingerprint authentication, read first and was stored.
[0056] Moreover, although the example which reads the fingerprint data registered into the storage section 38 to the degree of authentication at the storage section 40 was explained, you may make it read all the fingerprint data registered first here.
[0057] Furthermore, when there are already no fingerprint data registered at Step a8 that what is necessary is just to perform the error message of Step a9 if needed, you may progress to Step a1 immediately.
[0058] Drawing 5 is a flow chart which shows the 2nd operation of 31 for an information processor. This flow chart adds Steps a10 and a11 to the flow chart of drawing 4 , and explanation of the same step is omitted. When it judges whether the fingerprint is in agreement and is in agreement at Step a7, it progresses to Step a10. At Step a10, it judges whether there are any related data corresponding to the user of the fingerprint which was in agreement among the related data registered into the storage section 38. It progresses to Step a11 at a certain time, and these related data are read. And the operating environment and use function based on these related data are set up, a power supply ON state is maintained, and operation is ended. When there are no related data, a power supply ON state as it is is maintained, and operation is ended.
[0059] Drawing 6 is a flow chart which shows the 3rd operation of an information processor 31. Screen 71 to which the input of a personal identification number as shown in a display and the data reading screen 59 of a display and the fingerprint read station 34 at drawing 7 is urged is set up and expressed as Step a21. The personal identification number input area 72 for specifying the numeric value to 0-9, and inputting a personal identification number is set to Screen 71. In addition, this field 72 is also a fingerprint input area. At the following step a22, the central-process section 32 judges whether the alter operation of the personal identification number by contact of the finger to the personal identification number input area 72 of Screen 71 occurred. A finger is contacted to a field 72, and if it judges that the alter operation of a personal identification number occurred, it will progress to the following step a23. Here, a fingerprint is also inputted simultaneously with the input of a personal identification number. Moreover, contact of the finger to fields other than field 72 is disregarded.
[0060] At Step a23, the fingerprint data sensing control section 33 reads the coordinate data of the position where fingerprint data and the finger were contacted from a display and the fingerprint read station 34, and stores it temporarily in the storage section 58. At the following step a24, a personal identification number is detected and acquired based on the position by the acquired coordinate data. The acquired fingerprint data are stored in the storage section 40 at the following step a25. At the following step a26, it judges whether the input of a personal identification number was performed to the number of digits defined beforehand, for example, 4 figures. When inputted, it progresses to Step a27, and when not inputted, it returns to Step a22.
[0061] At Step a27, the central-process section 32 judges whether the acquired personal identification number and the personal identification number registered beforehand are collated and attested, and both are in agreement. When in agreement, it progresses to Step a28, and when not in agreement, it progresses to Step a29. At Step a28 whose personal identification number corresponded, the central-process section 32 judges whether the fingerprint data beforehand remembered to be acquired fingerprint data are collated and attested, and both are in agreement. When in agreement, operation is ended as it is, and when not in agreement, it progresses to Step a30. At Steps a29 and a30, an error message is performed and operation is ended.
[0062] In addition, like the aforementioned fingerprint authentication program, the authentication program of a personal identification number is read from the storage section 38, and is stored in the storage section 40. You may repeat and use the program which did not need to read and store this program in the degree of authentication of a personal identification number, either, read first and was stored. moreover, the error message of Steps a29 and a30 -- the need -- responding -- carrying out -- ****ing -- Step a -- you may end operation immediately after the end of 27 and 28 of operation
[0063] Drawing 8 is a flow chart which shows the 4th operation of an information processor 31. Screen 73 to which the input of a fingerprint as shown in a display and the data reading screen 59 of a display and the fingerprint read station 34 at drawing 9 is urged is set up and expressed as Step a41. Two or more fingerprint input frames 74 are set to Screen 73. Moreover, the fingerprint data memorized by the storage section 38 are read, and it is stored in the storage section 40.
[0064] At the following step a42, the central-process section 32 judges whether the alter operation of the fingerprint by contact of the finger into the fingerprint input frame 74 of Screen 73 occurred. A finger is contacted in a frame 74, and if it judges that the alter operation of a fingerprint occurred, it will progress to the following step a43. Here, contact of the finger to the outside of a frame 74 is disregarded.
[0065] At Step a43, the fingerprint data sensing control section 33 reads the coordinate data of the position where fingerprint data and the finger were contacted from a display and the fingerprint read station 34, and stores it temporarily in the storage section 58. At the following step a44, the inputted frame 74 is detected and acquired based on the position by the acquired coordinate data. The acquired fingerprint data are stored in the storage section 40 at the following step a45. At the following step a46, it judges whether **** with the fingerprint input and **** registered beforehand are collated and attested, and both are in agreement. When in agreement, it

progresses to Step a47, and when not in agreement, it progresses to Step a48.
[0066] At Step a47, the central-process section 32 judges whether all **** registered beforehand were collated and attested. When all are collated and it attests, operation is ended as it is, and when collating all and having not attested, it returns to Step a42. At Step a48, an error message is performed and operation is ended.
[0067] In addition, like the aforementioned fingerprint authentication program, the authentication program of **** is read from the storage section 38, and is stored in the storage section 40. You may repeat and use the program which did not need to read and store this program in the degree of authentication of ****, either, read first and was stored. Moreover, that what is necessary is just to carry out if needed, the error message of Step a48 may end operation immediately, when **** is not in agreement at Step a46.
[0068] Drawing 10 is a flow chart which shows the 5th operation of an information processor 31. Screen 75 to which the input of a fingerprint as shown in a display and the data reading screen 59 of a display and the fingerprint read station 34 at drawing 11 is urged is set up and expressed as Step a51. The fingerprint input frame 76 for every finger is set to Screen 75. Moreover, the fingerprint data memorized by the storage section 38 are read, and it is stored in the storage section 40.
[0069] At the following step a52, the central-process section 32 judges whether the alter operation of the fingerprint by contact of the finger into the fingerprint input frame 76 of Screen 75 occurred. A finger is contacted in a frame 76, and if it judges that the alter operation of a fingerprint occurred, it will progress to the following step a53. Here, contact of the finger to the outside of a frame 76 is disregarded.
[0070] At Step a53, the fingerprint data sensing control section 33 reads the coordinate data of the position where fingerprint data and the finger were contacted from a display and the fingerprint read station 34, and stores it temporarily in the storage section 58. At the following step a54, the inputted frame 76 is detected and acquired based on the position by the acquired coordinate data, and labeling of of which finger to be fingerprint data is performed. At the following step a55, each acquired fingerprint data by which labeling was carried out is stored in the storage section 40.
[0071] At the following step a56, it judges whether each fingerprint data by which labeling was carried out, and the fingerprint data registered beforehand are collated and attested, and both are in agreement. Moreover, it judges whether **** with the fingerprint input and **** registered beforehand are collated and attested, and both are in agreement. Here, even if a fingerprint and **** may judge the both and judge either, they are not cared about. When a fingerprint and/or **** are in agreement, operation is ended as it is, when not in agreement, it progresses to Step a57, an error message is performed, and operation is ended.
[0072] In addition, that what is necessary is just to carry out if needed, the error message of Step a57 may end operation immediately, when a fingerprint and/or **** are not in agreement at Step a56.
[0073] Drawing 12 is a flow chart which shows the 6th operation of an information processor 31. This flow chart deletes Steps a54-a57 of the flow chart of drawing 10 , Steps a58-a61 are added, and explanation of the same step is omitted. It judges whether if the fingerprint data sensing control section 33 reads the coordinate data of the position where fingerprint data and the finger were contacted from a display and the fingerprint read station 34, stores it temporarily in the storage section 58 and is transmitted to the storage section 40, at the following step a58, fingerprint data are collated and attested and it is in agreement with Step a53. When in agreement, it progresses to Step a59, and when not in agreement, it progresses to Step a61.
[0074] At Step a59, it judges whether the related data corresponding to the user of congruous fingerprint data are memorized. When memorizing, it progresses to Step a60, and the command by related data beforehand set up for every finger is read and executed, and operation is ended. When related data are not memorized, operation is ended as it is. At Step a61, an error message is performed and operation is ended.
[0075] In addition, that what is necessary is just to carry out if needed, the error message of Step a61 may end operation immediately, when fingerprint data are not in agreement at Step a58.
[0076] Drawing 13 is a flow chart which shows the 7th operation of an information processor 31. Screen 77 to which specification of an icon as shown in a display and the data reading screen 59 of a display and the fingerprint read station 34 at drawing 14 is urged is set up and expressed as Step a71. Two or more icons 78a-78f are set to Screen 77. In addition, a these icons [78a-78f] field is also a fingerprint input area. Moreover, the fingerprint data memorized by the storage section 38 are read, and it is stored in the storage section 40.
[0077] At the following step a72, the central-process section 32 judges whether the alter operation of the fingerprint by contact of the finger to Screen 77 occurred. A finger is contacted, and if it judges that the alter operation of a fingerprint occurred, it will progress to the following step a73. It is also possible to control by contact of the finger to the outside of icon 78a-78f here not to progress to the next processing.
[0078] At Step a73, the fingerprint data sensing control section 33 reads the coordinate data of the position where fingerprint data and the finger were contacted from a display and the fingerprint read station 34, stores it temporarily in the storage section 58, and is transmitted to the storage section 40. At the following step a74, fingerprint data are collated and attested and it judges whether it is in agreement. When in agreement, it progresses to Step a75, when not in agreement, it progresses to Step a80, and an error message is performed, and operation is ended.
[0079] At Step a75, it judges in which icon 78a-78f the fingerprint input was made. At the time of telephone directory icon 78a, it progresses to Step a79 at Step a76, respectively at the time of schedule icon 78b for application icon 78d to solve to Step a78 to Step a77 at the time of file management icon 78c. Although there is nothing to this flow chart, the application of a voice memorandum of the application of a handwriting memorandum at the time of icon 78f is started at the time of icon 78e, and it is completed. At the time besides icon 78a-78f, operation is ended as it is. Operation is ended at Steps a76-a78, reading and displaying only the data of the user of a fingerprint with whom the application corresponding to each specified icons 78a-78c was in agreement, and using data editing, such as registration, change, and deletion, as possible. Moreover, at Step a79, the application corresponding to the user of a fingerprint with whom it was [in the application beforehand registered for every user] in agreement is started, and operation is ended.
[0080] In addition, that what is necessary is just to carry out if needed, the error message of Step a80 may end operation immediately, when fingerprint data are not in agreement at Step a74.

[0081] Drawing 15 is a flow chart which shows the 8th operation of an information processor 31. Screen 79 to which specification of a menu as shown in a display and the data reading screen 59 of a display and the fingerprint read station 34 at drawing 16 is urged is set up and expressed as Step a81. Here, a menu is two, a machine setup and network connection, and two menu appointed fields 80a and 80b are set to the aforementioned screen 79. In addition, these menu appointed fields 80a and 80b are also fingerprint input areas. Moreover, the fingerprint data memorized by the storage section 38 are read, and it is stored in the storage section 40.
[0082] The menu appointed fields 80a and 80b of the aforementioned screen 79 to which menu specification is urged are classified into two or more field A-J as concretely shown in drawing 17 . The authority level at the time of menu execution is specified to be which field A-J in Fields 80a and 80b by whether the fingerprint input was made.
[0083] At the following step a82, the central-process section 32 judges whether the alter operation of the fingerprint by contact of the finger to Screen 79 occurred. A finger is contacted, and if it judges that the alter operation of a fingerprint occurred, it will progress to the following step a83. It is also possible to control by contact of the finger to the outside of menu appointed field 80a and 80b here not to progress to the next processing.
[0084] At Step a83, the fingerprint data sensing control section 33 reads the coordinate data of the position where fingerprint data and the finger were contacted from a display and the fingerprint read station 34, stores it temporarily in the storage section 58, and is transmitted to the storage section 40. At the following step a84, fingerprint data are collated and attested and it judges whether it is in agreement. When in agreement, it progresses to Step a85, when not in agreement, it progresses to Step a90, and an error message is performed, and operation is ended.
[0085] At Step a85, the authority data corresponding to the user of the congruous fingerprints are read from the storage section 38, and it stores in the storage section 40. At the following step a86, it judges in which field A-E the fingerprint input was made. As the menu of a machine setup is performed on the authority level which is the level of the authority data which progressed to Step a88 at the time of Fields B or D, progressed to Step a89, respectively at the time of Fields C or E, and were read and stored at the time of Field A, and is specified to be Step a87 by each field A-E, operation is ended, and at the times other than this, operation is ended as it is.
[0086] In addition, that what is necessary is just to carry out if needed, the error message of Step a90 may end operation immediately, when fingerprint data are not in agreement at Step a84.
[0087] Drawing 18 is a flow chart which shows the 9th operation of an information processor 31. This flow chart deletes step a87-89 of the flow chart of drawing 15 , and adds Steps a91-a93, and explanation of the same step is omitted. At Step a86, it judges in which field F-J the fingerprint input was made. As the menu of network connection is performed on the authority level which is the level of the authority data which progressed to Step a92 at the time of Fields G or I, progressed to Step a93, respectively at the time of Fields H or J, and were read and stored at the time of Field F, and is specified to be Step a91 by each field F-J, operation is ended, and at the times other than this, operation is ended as it is.
[0088] Drawing 19 is a flow chart which shows the 10th operation of an information processor 31. Screen 81 which has the report 83 as shown in a display and the data reading screen 59 of a display and the fingerprint read station 34 at drawing 20 is set up and expressed as Step a101. The seal column 82 is set to the report 83. In addition, this seal column 82 is also a fingerprint input area. Moreover, the fingerprint data memorized by the storage section 38 are read, and it is stored in the storage section 40.
[0089] At the following step a102, the central-process section 32 judges whether the alter operation of the fingerprint by contact of the finger to a report 83 occurred. A finger is contacted by the report 83, and if it judges that the alter operation of a fingerprint occurred, it will progress to the following step a103. Here, contact of a finger may be the whole screen 81.
[0090] At Step a103, the fingerprint data sensing control section 33 reads the coordinate data of the position where fingerprint data and the finger were contacted from a display and the fingerprint read station 34, stores it temporarily in the storage section 58, and is transmitted to the storage section 40. At the following step a104, it judges whether the input of a fingerprint was made into the seal column 82. when it is in the seal column 82, it progresses to Step a105, and when it comes out other than this and is, it progresses to Step a111, an error message is performed, and operation is ended
[0091] At Step a105, fingerprint data are collated and attested and it judges whether it is in agreement. When in agreement, it progresses to Step a106, when not in agreement, it progresses to Step a111, and an error message is performed, and operation is ended.

[0092] At Step a106, congruous fingerprint data judge whether you are the seal authority owner of a report based on related data. When a judgment result is affirmation, it progresses to Step a107, and when it is negative, the purport which progresses to Step a110 and does not have recognition authority is displayed, and operation is ended.
[0093] At Step a107, it judges whether the next seal person is set as the report. When set up, it progresses to Step a108, and when not set up, it progresses to Step a109. At Step a108, the report with which a fingerprint input person's recognition mark was added to the report, and the recognition mark was added is circulated to the next seal person. That is, data transmission is carried out through a network at the next seal person. And operation is ended. At Step a109, the report with which a fingerprint input person's recognition mark was added to the report, and the recognition mark was added is kept to the storage area set as the report file, and operation is ended.
[0094] In addition, that what is necessary is just to carry out if needed, the display of Step a110 and the error message of Step a111 may end operation immediately, when judgment is negative at the time of fingerprint data not being in agreement at Step a105, or Step a106.
[0095] Drawing 21 is a flow chart which shows the 11th operation of an information processor 31. Screen 84 which has settlement-of-accounts ****** 86 as shown in a display and the data reading screen 59 of a display and the fingerprint read station 34 at drawing 22 is set up and expressed as Step a121. The seal column 85 is set to settlement-of-accounts ****** 86. In addition, this seal column 85 is also a fingerprint input area. Moreover, the fingerprint data memorized by the storage section 38 are read, and it is stored in the storage section 40.
[0096] At the following step a122, the central-process section 32 judges whether the alter operation of the fingerprint by contact of the finger to settlement-of-accounts ****** 86 occurred. A finger is contacted by settlement-of-accounts ****** 86, and if it judges that

the alter operation of a fingerprint occurred, it will progress to the following step a123. Here, contact of a finger may be the whole screen 84.
[0097] At Step a123, the fingerprint data sensing control section 33 reads the coordinate data of the position where fingerprint data and the finger were contacted from a display and the fingerprint read station 34, stores it temporarily in the storage section 58, and is transmitted to the storage section 40. At the following step a124, it judges whether the input of a fingerprint was made into the seal column 85. when it is in the seal column 85, it progresses to Step a125, and when it comes out other than this and is, it progresses to Step a131, an error message is performed, and operation is ended
[0098] At Step a125, fingerprint data are collated and attested and it judges whether it is in agreement. When in agreement, it progresses to Step a126, when not in agreement, it progresses to Step a131, and an error message is performed, and operation is ended.

[0099] At Step a126, congruous fingerprint data judge whether you are the seal authority owner of settlement-of-accounts ****** based on related data. When a judgment result is affirmation, it progresses to Step a127, and when it is negative, the purport which progresses to Step a130 and does not have recognition authority is displayed, and operation is ended.
[0100] At Step a127, the total amount of money of settlement-of-accounts ****** judges whether it is the inside of a recognition person's sanction authority. When it is in authority, it progresses to Step a129, and when it is not in authority, it progresses to Step a128. At Step a128, it circulates to the recognition person of settlement-of-accounts recognition **** to which a fingerprint input person's recognition mark was added to settlement-of-accounts ******, and the recognition mark was added. That is, data transmission is carried out through a network at the next recognition person. And operation is ended. At Step a129, settlement-of-accounts ****** to which a fingerprint input person's recognition mark was added to settlement-of-accounts ******, and the recognition mark was added is kept to the storage area set as the settlement-of-accounts ****** file, issue processing of an order sheet is performed further, and operation is ended.
[0101] In addition, that what is necessary is just to carry out if needed, the display of Step a130 and the error message of Step a131 may end operation immediately, when judgment is negative at the time of fingerprint data not being in agreement at Step a125, or Step a126.
[0102] Drawing 23 is the block diagram of the information processor 57 which are other forms of operation of this invention. Although an information processor 57 is constituted almost like the aforementioned information processor 31, it has a mouse 52 as a coordinate specification means, and is characterized by forming the reading side 50 of a fingerprint read station in this mouse 52. The same reference mark is attached and shown in the same component as the aforementioned equipment 31.
[0103] In the central-process section 32 of the information processor 57 equipped with a fingerprint authentication function With the fingerprint data sensing control section 49 which controls fingerprint reading operation, the display-control section 36 which controls the display action of a display 51, the pointer control section 55 which controls operation of a mouse 52, and a mouse The fingerprint reading station detecting element 56 and the key input section 37 which detect the coordinate position relevant to the fingerprint read on the screen specified, the storage section 38, the I/O section 39, and the storage section 40 are connected, and operation of the whole equipment is controlled in generalization.
[0104] A liquid crystal display realizes and a display 51 has the screen to which rectangular coordinates were set. Well-known technology realizes and a fingerprint read station has the fingerprint reading side 50 where a finger is contacted. On the other hand, inside [it is the right-and-left buttons 53 and 54 which this fingerprint reading side 50 is formed in the front face of a mouse 52, for example, a mouse 52 has] is formed in the left button 53 a button and here. Based on the coordinate data detected and acquired by the fingerprint reading station detecting element 56, the central-process section 32 controls operation of an information processor 57 like the aforementioned information processor 31, and controls operation of equipment 57 like the aforementioned equipment 31 based on the acquired fingerprint data.
[0105]
[Effect of the Invention] As mentioned above, according to this invention, it sets to an information processor equipped with a fingerprint authentication function, and the motion control of an information processor based on a coordinate becomes possible by easy operation of the coordinate specification relevant to the fingerprint read on the screen at the time of fingerprint authentication.
[0106] Moreover, according to this invention, since the screen and the fingerprint reading side were made the same, fingerprint input and coordinate specification can be performed by the same operation, and high operability is acquired.
[0107] Moreover, according to this invention, since the fingerprint reading side was formed in the coordinate specification means, coordinate specification and a fingerprint input can be performed by the same operation, and high operability is acquired.
[0108] Moreover, since according to this invention it was made to perform fingerprint authentication only when a specific coordinate was specified, high security nature can be obtained.
[0109] Moreover, according to this invention, it sets to an information processor equipped with a fingerprint authentication function, and the coordinate relevant to the fingerprint read on the screen at the time of fingerprint authentication is specified, and a personal identification number is acquired from the specified coordinate. The acquired personal identification number is attested and the motion control of an information processor based on the authentication result of a personal identification number of it becomes possible. Thus, operation of an information processor is controllable by the easy operation of the coordinate specification for the personal identification number input at the time of fingerprint authentication.
[0110] Moreover, since according to this invention it was made to perform fingerprint authentication only when the personal identification number was in agreement, high security nature can be obtained.
[0111] Moreover, since according to this invention operation of the power supply of an information processor was controlled when the fingerprint was in agreement, high security nature and high operability can be acquired, and reduction of power consumption can be aimed at.
[0112] Moreover, since the operating condition corresponding to the user of the fingerprint which was in agreement out of the operating condition beforehand set up for every user is read and it was made to set up according to this invention when the fingerprint

was in agreement, the operating environment and the use function to have been suitable for the user can be set up, and high operability is acquired.

[0113] Moreover, according to this invention, since fingerprint authentication of each finger was enabled in the fingerprint authentication function, the fine motion control of an information processor based on the fingerprint authentication result of each finger becomes possible.

[0114] Moreover, since it was made to perform by reading the command corresponding to each finger of the user of the congruous fingerprints out of the command beforehand registered for every finger of a user based on the fingerprint authentication result of each finger according to this invention, high security nature and high operability can be acquired, and the fine motion control for every finger becomes possible.

[0115] Moreover, according to this invention, it sets to an information processor equipped with a fingerprint authentication function. When the coordinate was specified as it mentioned above, the motion control of an information processor based on the judgment result and fingerprint authentication result of icon specification is possible at this time, and an icon is specified and a fingerprint is in agreement, Only the data of the user of a fingerprint with whom the application corresponding to the specified icon was in agreement can be read and displayed, it can do in this way, and operation of an information processor can be controlled by easy operation.

[0116] Moreover, when according to this invention an icon is specified and a fingerprint is in agreement, the application corresponding to the user of a fingerprint with whom it was [in the application beforehand set up for every user] in agreement can be started, it can do in this way, and operation of an information processor can be controlled by easy operation.

[0117] Moreover, when according to this invention an icon is specified and a fingerprint is in agreement, only the file of the user of a fingerprint which corresponded can be opened, it can do in this way, and operation of an information processor can be controlled by easy operation.

[0118] Moreover, according to this invention, it sets to an information processor equipped with a fingerprint authentication function. When the coordinate was specified as it mentioned above, the motion control of an information processor based on the judgment result and fingerprint authentication result of a menu runlevel block definition is possible at this time, and a menu runlevel field is specified and a fingerprint is in agreement, It is a runlevel corresponding to the user of a fingerprint with whom it was [in the runlevel beforehand set up for every user] in agreement, and a menu can be performed by the runlevel of the specified menu runlevel field, it can do in this way, and operation of an information processor can be controlled by easy operation.

[0119] Moreover, when the coordinate in the seal column is specified to the documents which have the seal column according to this invention, the recognition mark is added, these documents communicate by means of communications, it can do in this way, and documents, such as a report, can be transmitted and circulated to the next man.

[0120] Moreover, when the coordinate in the seal column is specified to the documents which have the seal column according to this invention, the recognition mark can be added, an incidental means can be made by these documents, it can do in this way, and issue processing of an order sheet can be performed to documents, such as settlement-of-accounts ******.

[Translation done.]

* NOTICES *

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1] It is the block diagram of the information processor 31 which is one gestalt of operation of this invention.
[Drawing 2] It is drawing showing a display and the data reading screen 59 of a display and the fingerprint read station 34.
[Drawing 3] It is drawing showing the user registration data of the storage section 38.
[Drawing 4] It is the flow chart which shows the 1st operation of 31 for an information processor.
[Drawing 5] It is the flow chart which shows the 2nd operation of 31 for an information processor.
[Drawing 6] It is the flow chart which shows the 3rd operation of an information processor 31.
[Drawing 7] It is drawing showing Screen 71 to which the input of a personal identification number is urged.
[Drawing 8] It is the flow chart which shows the 4th operation of an information processor 31.
[Drawing 9] It is drawing showing Screen 73 to which the input of a fingerprint is urged.
[Drawing 10] It is the flow chart which shows the 5th operation of an information processor 31.
[Drawing 11] It is drawing showing Screen 75 to which the input of a fingerprint is urged.
[Drawing 12] It is the flow chart which shows the 6th operation of an information processor 31.
[Drawing 13] It is the flow chart which shows the 7th operation of an information processor 31.
[Drawing 14] It is drawing showing Screen 77 to which specification of an icon is urged.
[Drawing 15] It is the flow chart which shows octavus operation of an information processor 31.
[Drawing 16] It is drawing showing Screen 79 to which specification of a menu is urged.
[Drawing 17] It is drawing showing two or more field A-J of the menu appointed fields 80a and 80b of the aforementioned screen 79.
[Drawing 18] It is the flow chart which shows the 9th operation of an information processor 31.
[Drawing 19] It is the flow chart which shows the 10th operation of an information processor 31.
[Drawing 20] It is drawing showing Screen 81 which has a report 83.
[Drawing 21] It is the flow chart which shows the 11th operation of an information processor 31.
[Drawing 22] It is drawing showing Screen 84 which has settlement-of-accounts ****** 86.
[Drawing 23] It is the block diagram of the information processor 57 which are other gestalten of operation of this invention.
[Drawing 24] It is the block diagram of the information processor 1 of the conventional technology.
[Drawing 25] It is drawing showing the fingerprint read station 4 and display 7 of an information processor 1.
[Description of Notations]
31 57 Information processor
32 Central-Process Section
33 49 Fingerprint data sensing control section
34 Display and Fingerprint Read Station
35 Fingerprint Sensing Area Setting Section
36 Display-Control Section
38 40 Storage section
39 I/O Section
41 Program Work Memory
42 Fingerprint Authentication Section
43 Feature-Extraction Section
44 Collating Section
45 Fingerprint, Related Data Read-out, and Storing Section
46 Read-out Section
47 Storing Section
48 Application Program Storing Section
50 Fingerprint Reading Side
51 Display
52 Mouse
53 Left Button
54 Right Button
55 Pointer Control Section
56 Fingerprint Reading Station Detecting Element
58 Coordinate Position and Fingerprint Data-Storage Section
59 Display and Data Reading Screen

60 Fingerprint Reading Field

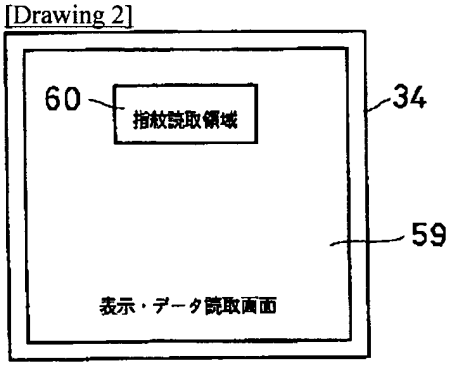
[Translation done.]

* NOTICES *

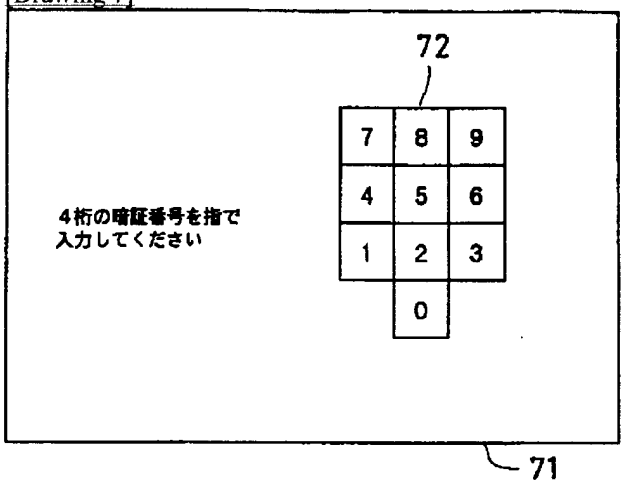
1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DRAWINGS

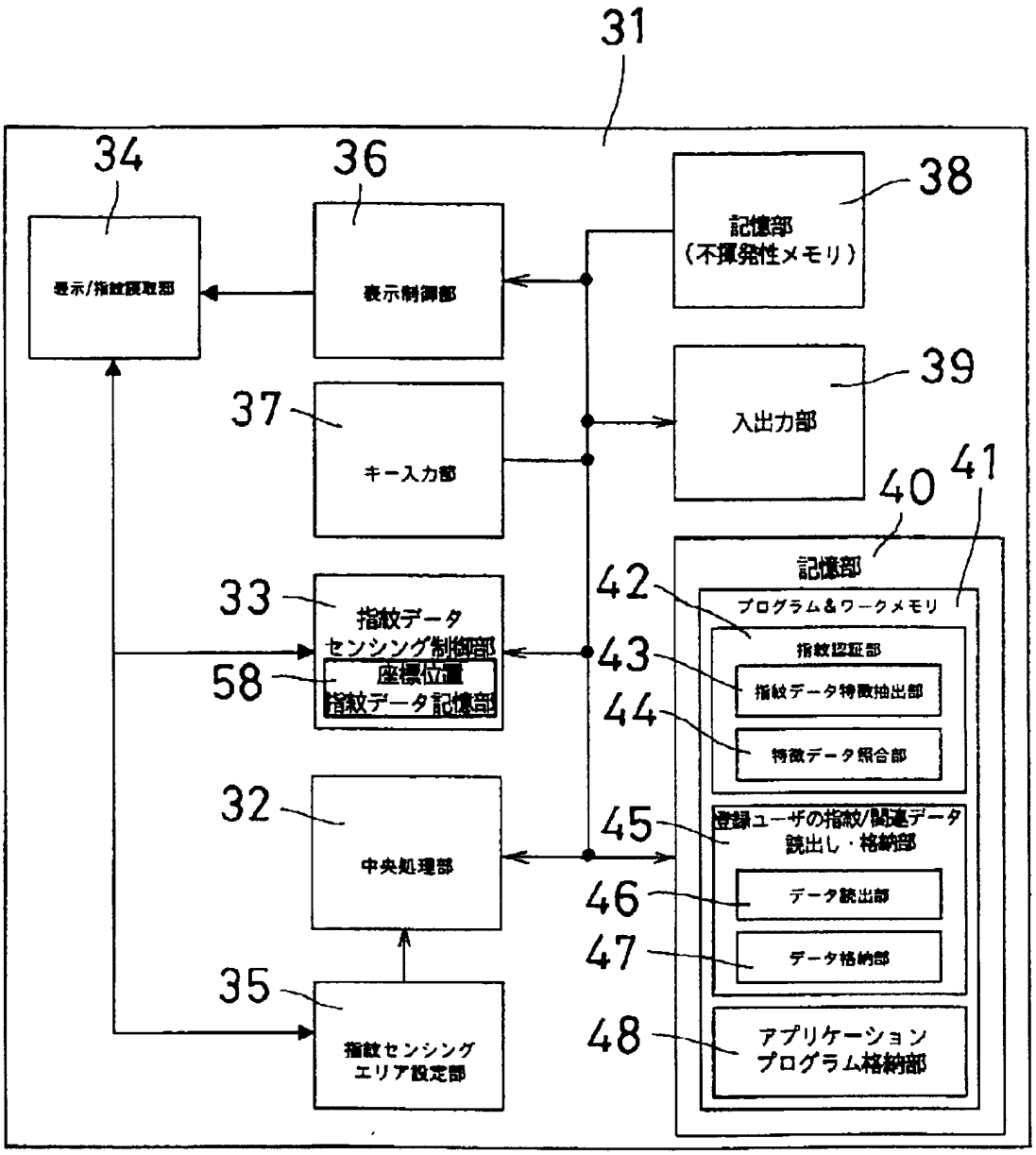
[Drawing 2]



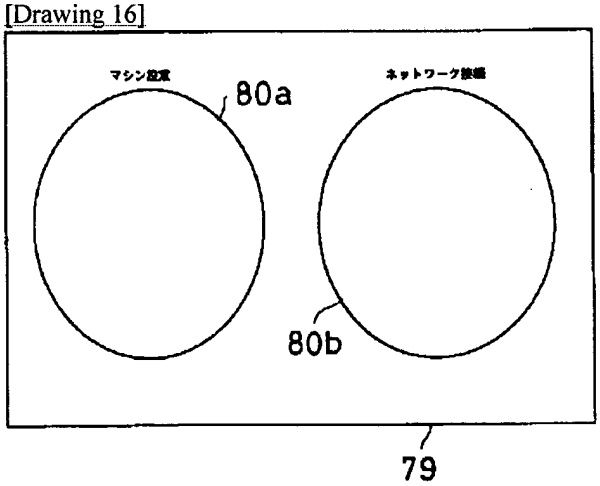
[Drawing 7]



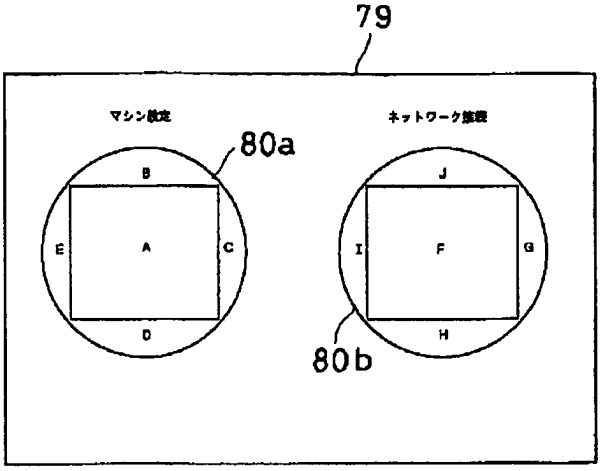
[Drawing 1]



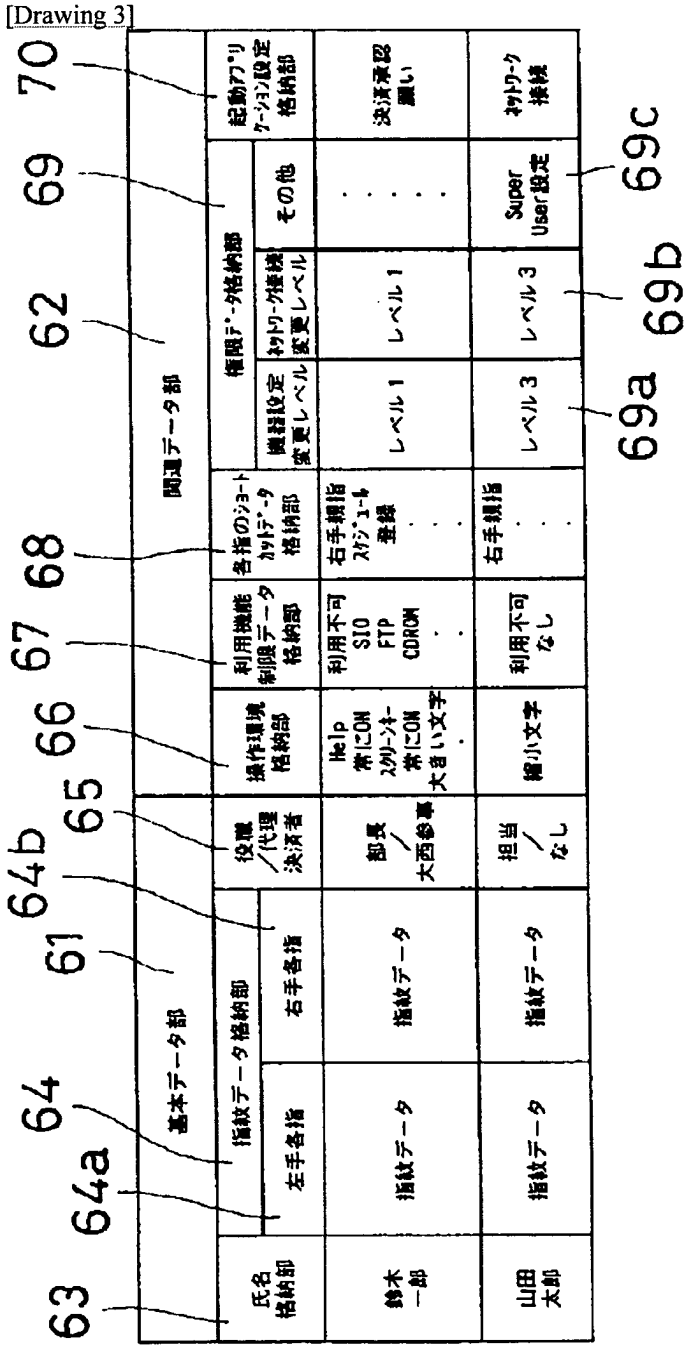
[Drawing 16]



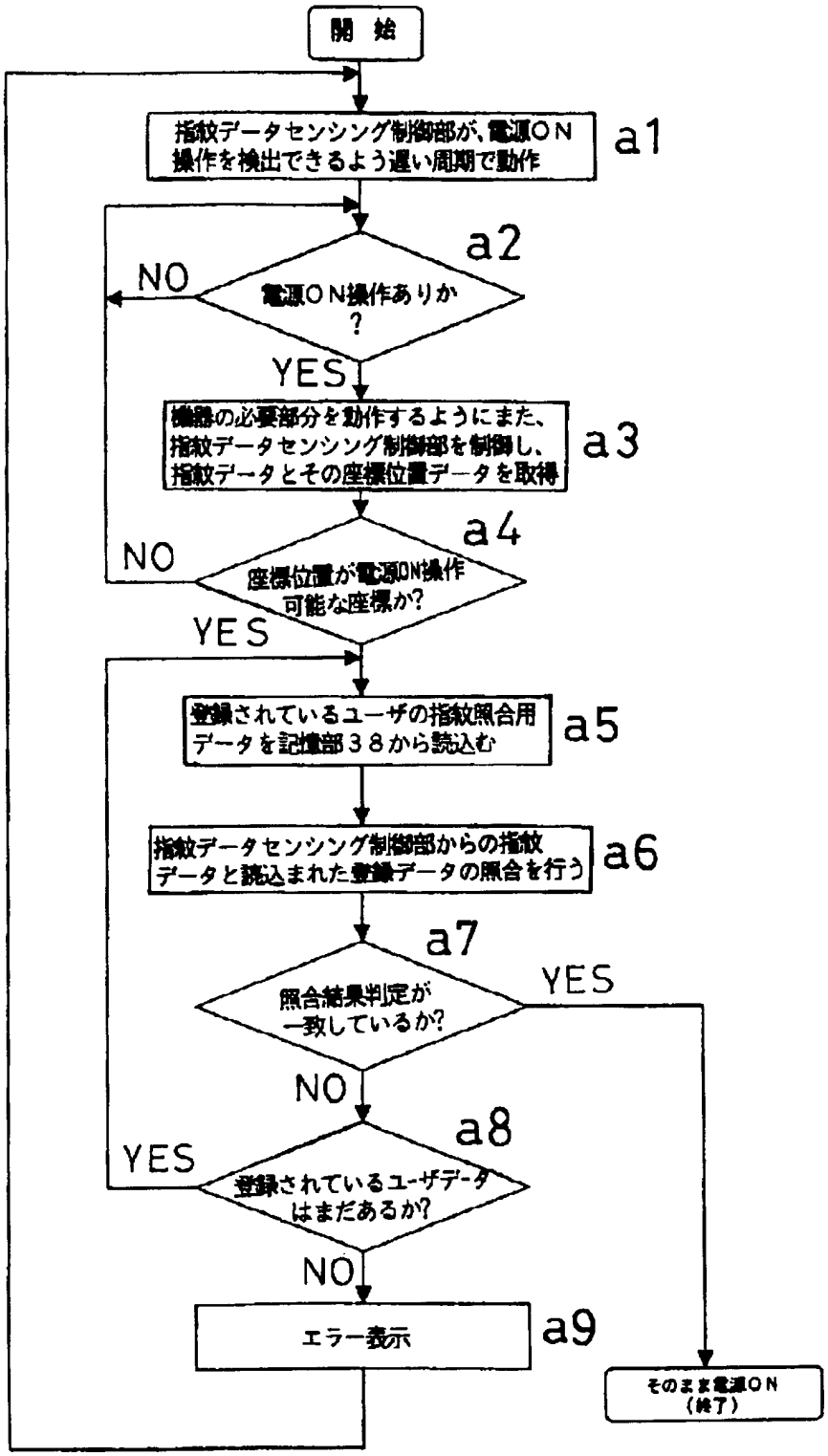
[Drawing 17]



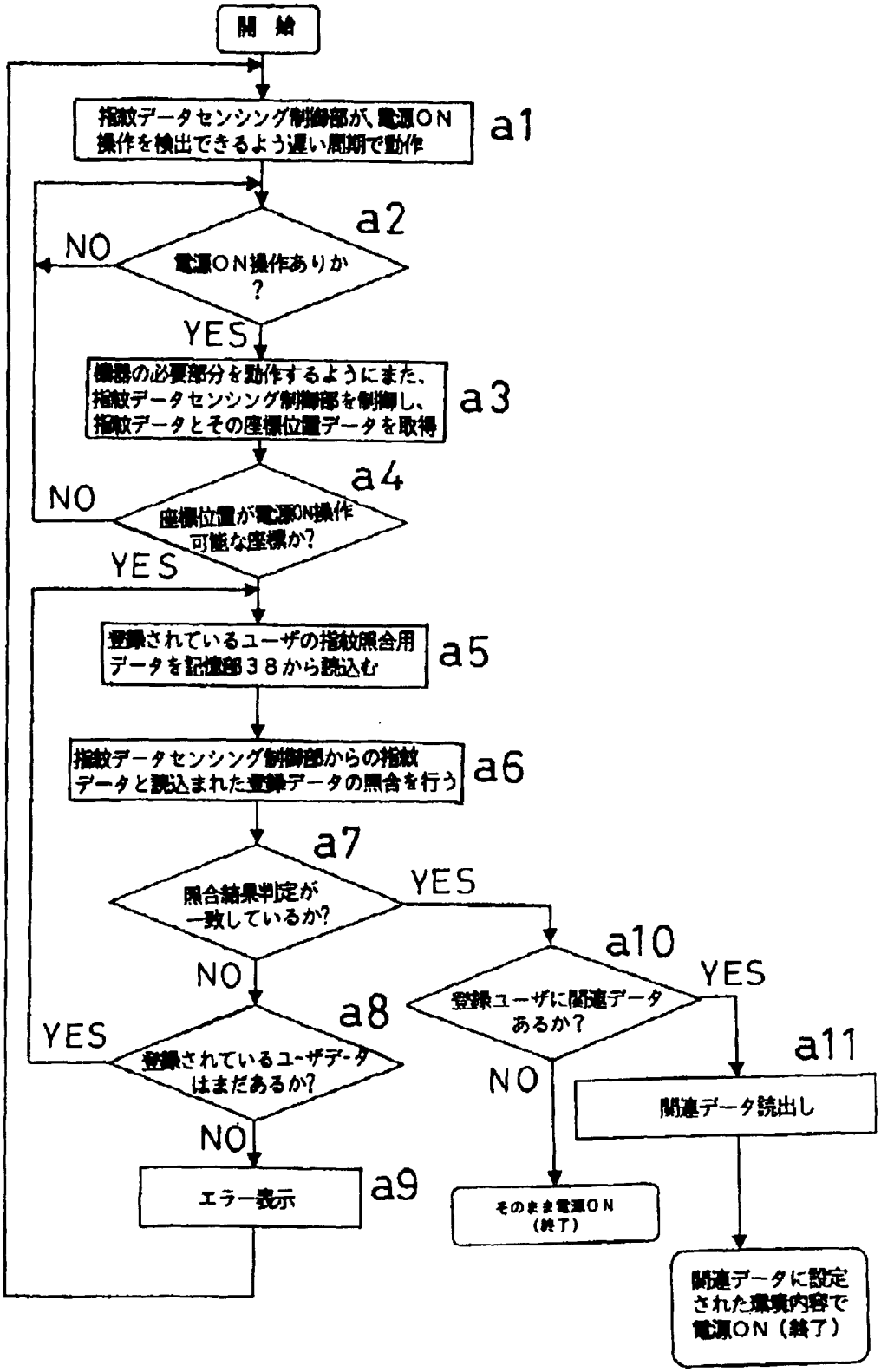
[Drawing 3]



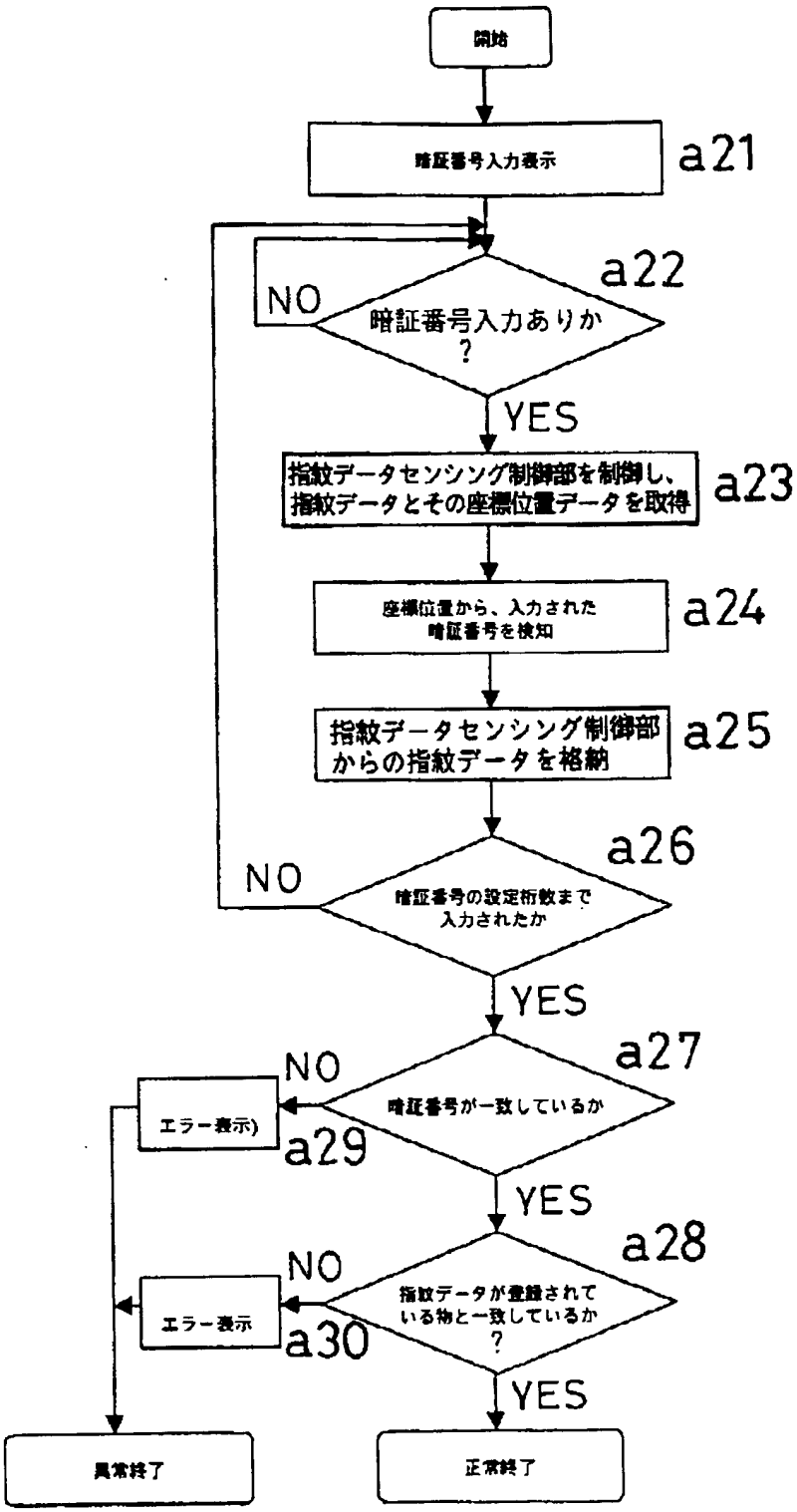
[Drawing 4]


開 始
指紋データセンシング制御部が、電源ON操作を検出できるよう遅い周期で動作
a1
a2
NO
電源ON操作ありか？
YES
機器の必要部分を動作するようにまた、指紋データセンシング制御部を制御し、指紋データとその座標位置データを取得
a3
a4
NO
座標位置が電源ON操作可能な座標か?
YES
登録されているユーザの指紋照合用データを記憶部３８から読込む
a5
指紋データセンシング制御部からの指紋データと読込まれた登録データの照合を行う
a6
a7
照合結果判定が一致しているか?
YES
NO
a8
YES
登録されているユーザデータはまだあるか?
NO
エラー表示
a9
そのまま電源ON（終了）

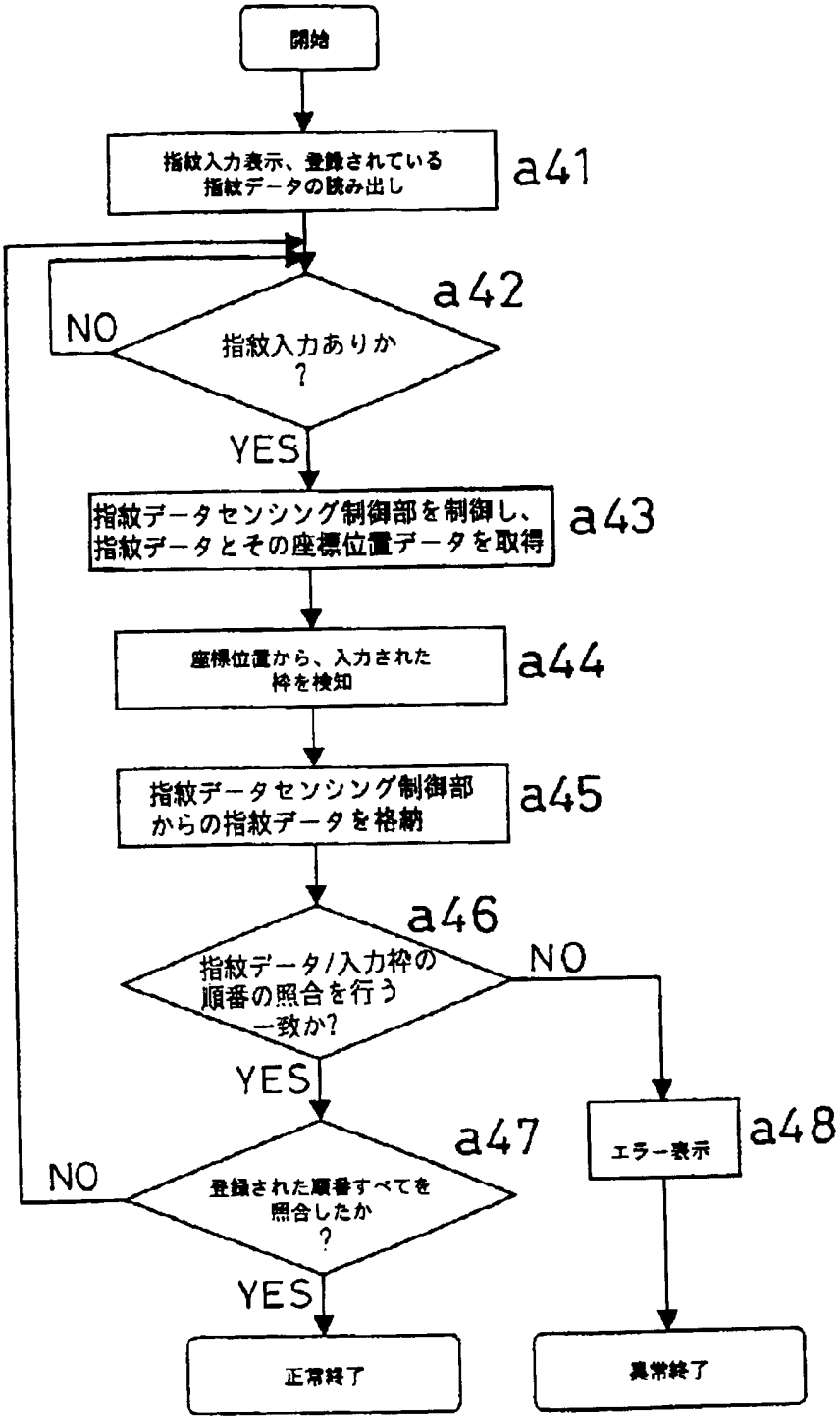
[Drawing 5]


開 始
指紋データセンシング制御部が、電源ON操作を検出できるよう遅い周期で動作
a1
a2
NO
電源ON操作ありか？
YES
機器の必要部分を動作するようにまた、指紋データセンシング制御部を制御し、指紋データとその座標位置データを取得
a3
a4
NO
座標位置が電源ON操作可能な座標か?
YES
登録されているユーザの指紋照合用データを記憶部３８から読込む
a5
指紋データセンシング制御部からの指紋データと読込まれた登録データの照合を行う
a6
a7
照合結果判定が一致しているか?
YES
NO
a8
YES
登録されているユーザデータはまだあるか?
NO
エラー表示
a9
a10
登録ユーザに関連データあるか?
YES
NO
a11
関連データ読出し
そのまま電源ON（終了）
関連データに設定された環境内容で電源ON（終了）

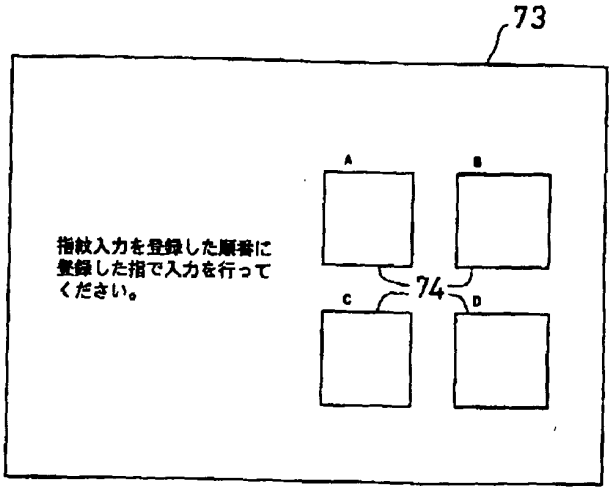
[Drawing 6]


開始
暗証番号入力表示
a21
a22
NO
暗証番号入力ありか
?
YES
指紋データセンシング制御部を制御し、
指紋データとその座標位置データを取得
a23
座標位置から、入力された
暗証番号を検知
a24
指紋データセンシング制御部
からの指紋データを格納
a25
a26
NO
暗証番号の設定桁数まで
入力されたか
YES
a27
NO
エラー表示)
a29
暗証番号が一致しているか
YES
a28
NO
エラー表示
a30
指紋データが登録されて
いる物と一致しているか
?
YES
異常終了
正常終了

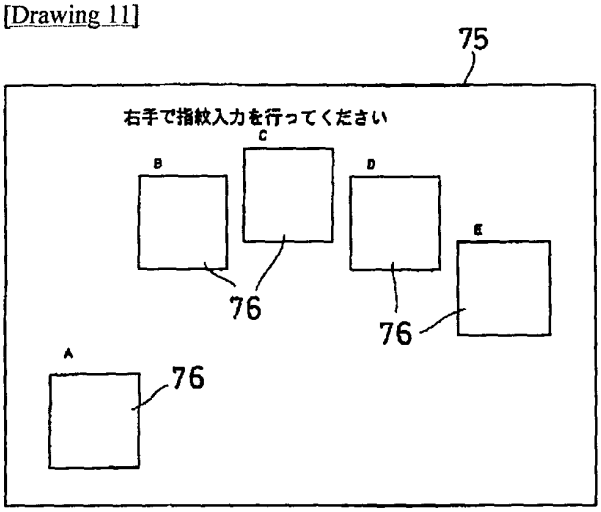
[Drawing 8]


開始
指紋入力表示、登録されている指紋データの読み出し
a41
a42
NO
指紋入力ありか?
YES
指紋データセンシング制御部を制御し、指紋データとその座標位置データを取得
a43
座標位置から、入力された枠を検知
a44
指紋データセンシング制御部からの指紋データを格納
a45
a46
指紋データ/入力枠の順番の照合を行う一致か?
NO
YES
a47
エラー表示
a48
NO
登録された順番すべてを照合したか?
YES
正常終了
異常終了

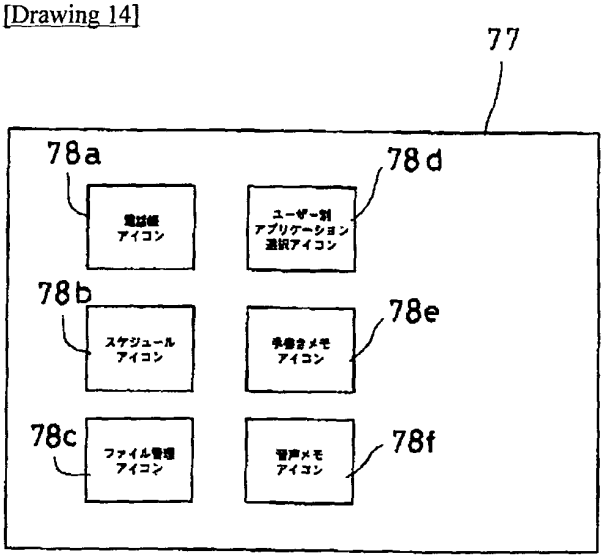
[Drawing 9]



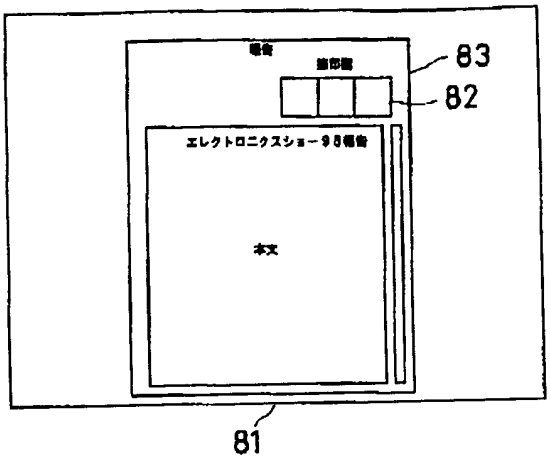
[Drawing 11]



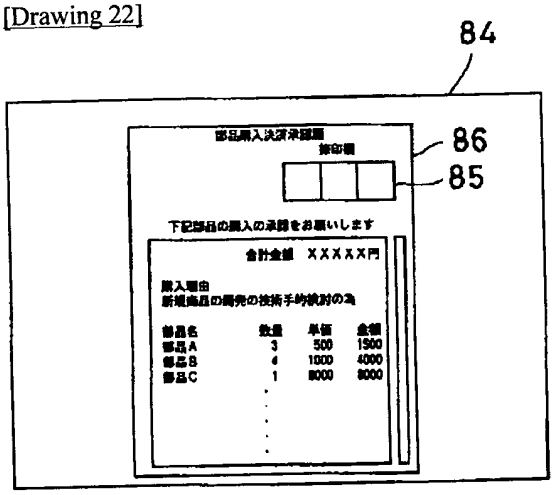
[Drawing 14]



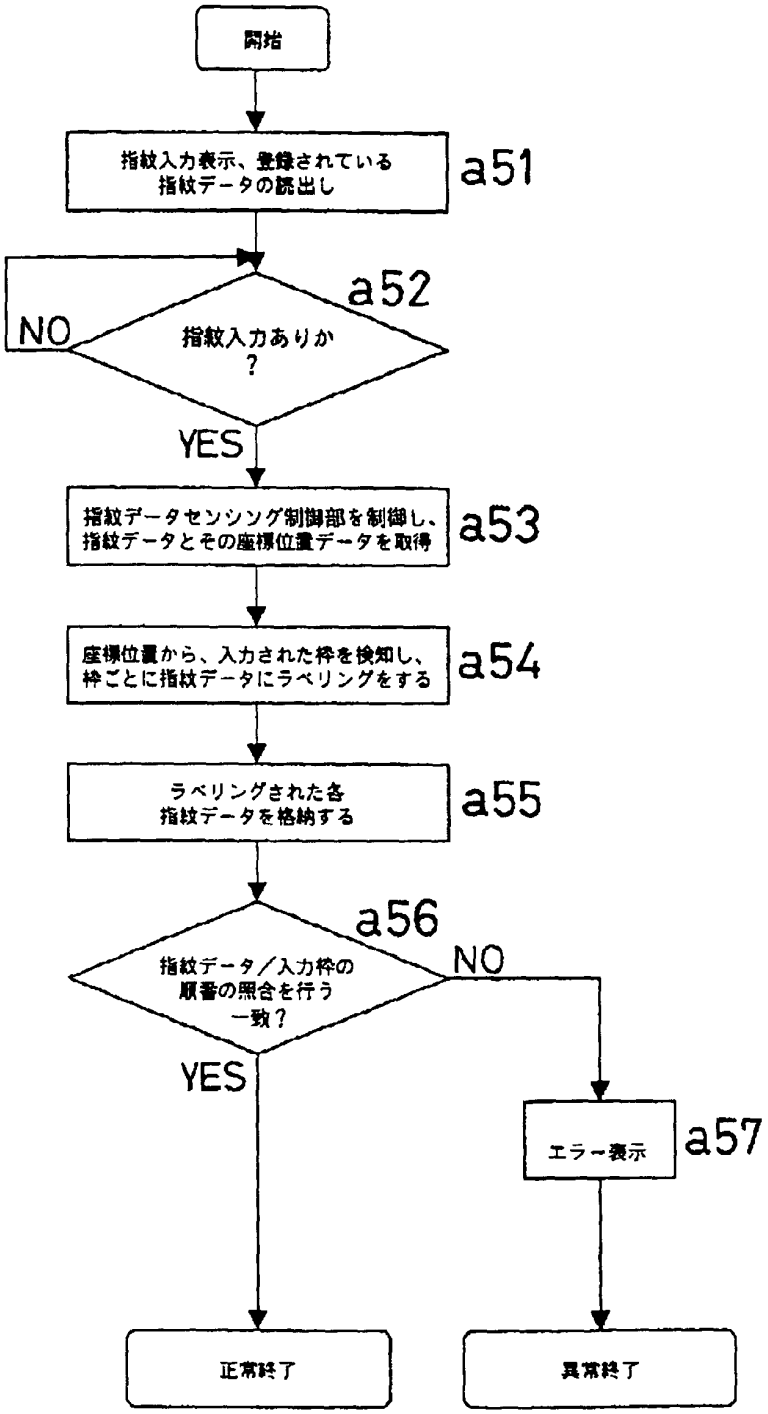
[Drawing 20]



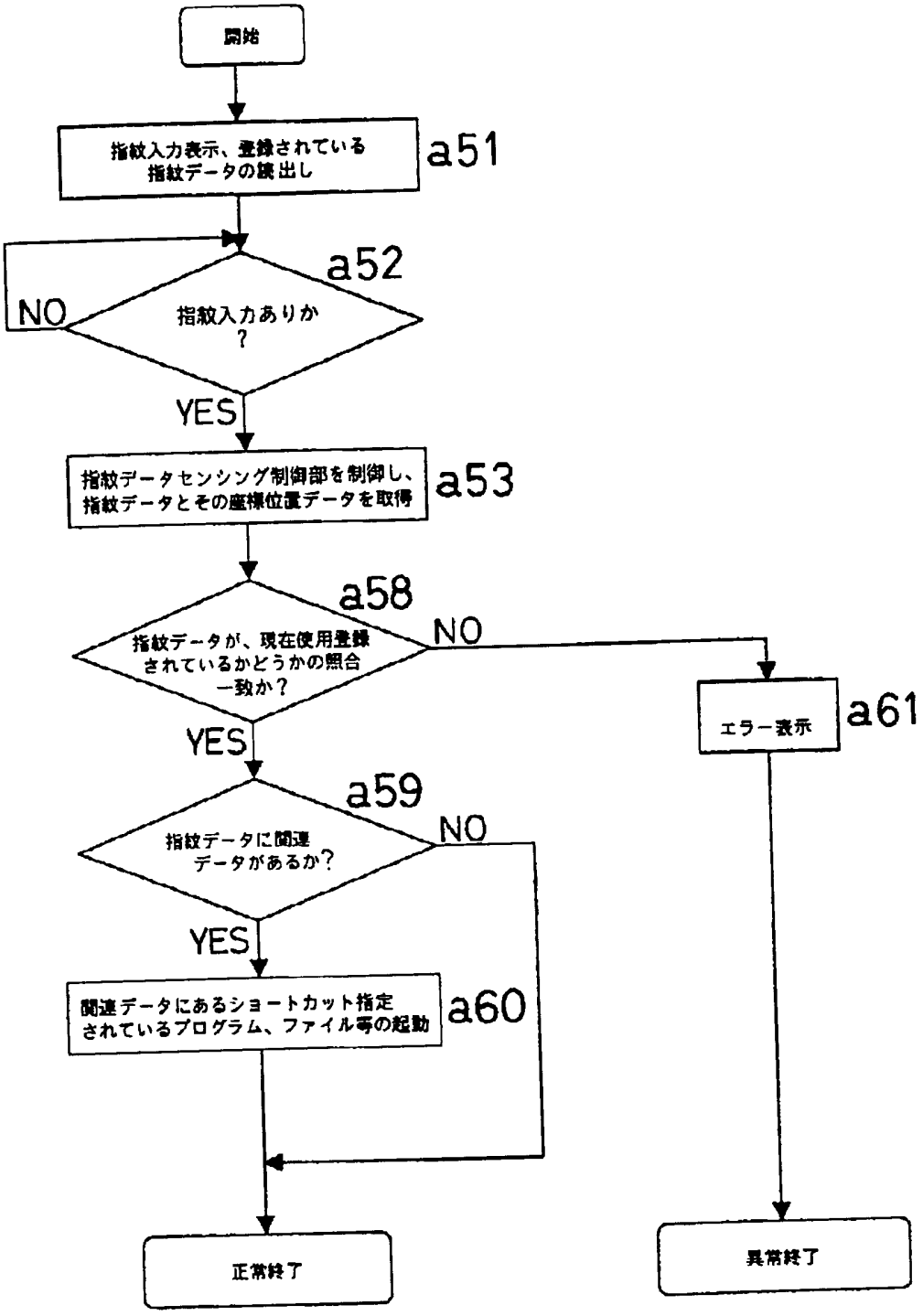
[Drawing 22]



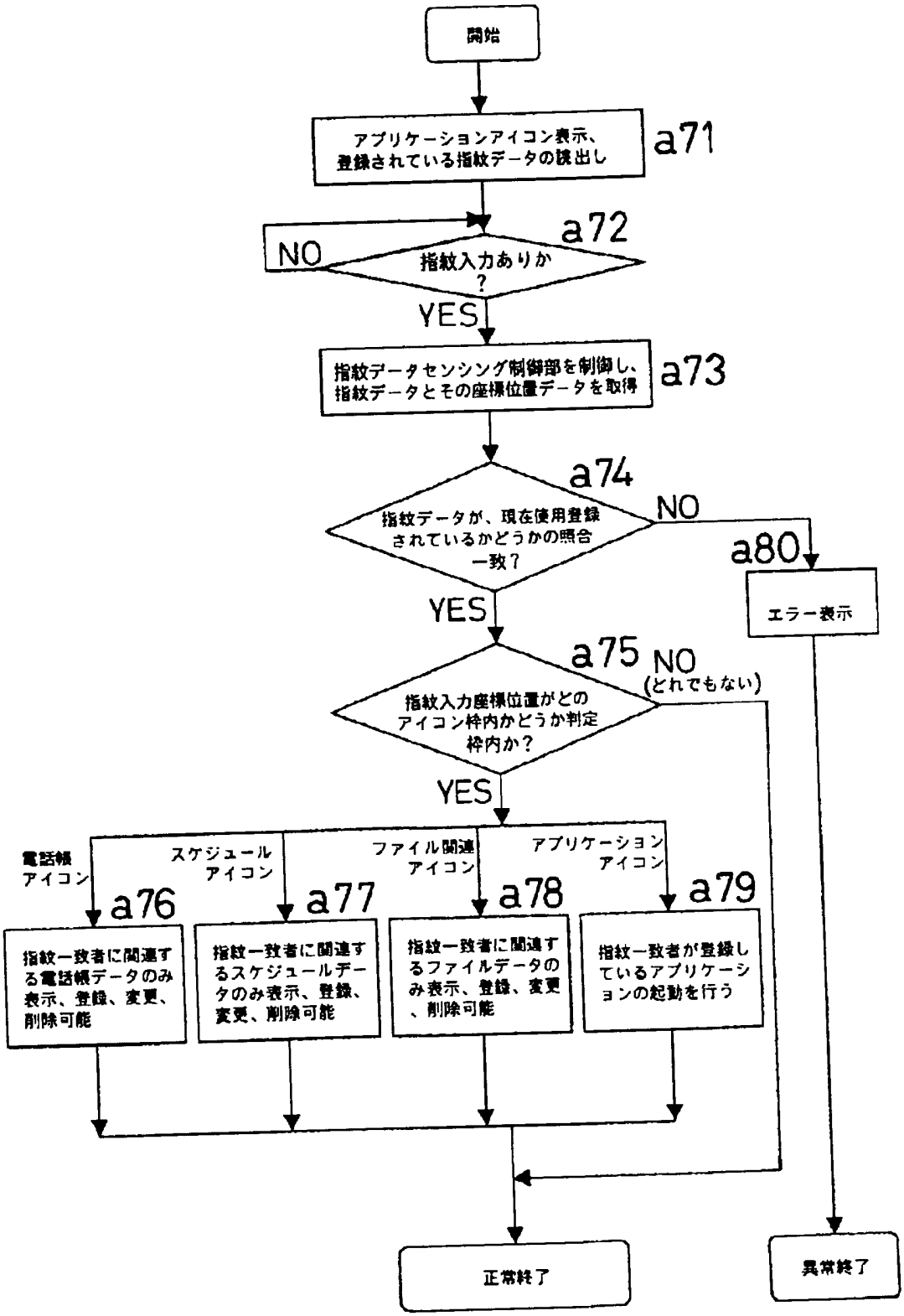
[Drawing 10]


開始
指紋入力表示、登録されている
指紋データの読出し
a51
a52
NO
指紋入力ありか
?
YES
指紋データセンシング制御部を制御し、
指紋データとその座標位置データを取得
a53
座標位置から、入力された枠を検知し、
枠ごとに指紋データにラベリングをする
a54
ラベリングされた各
指紋データを格納する
a55
a56
指紋データ／入力枠の
順番の照合を行う
一致？
NO
YES
エラー表示
a57
正常終了
異常終了

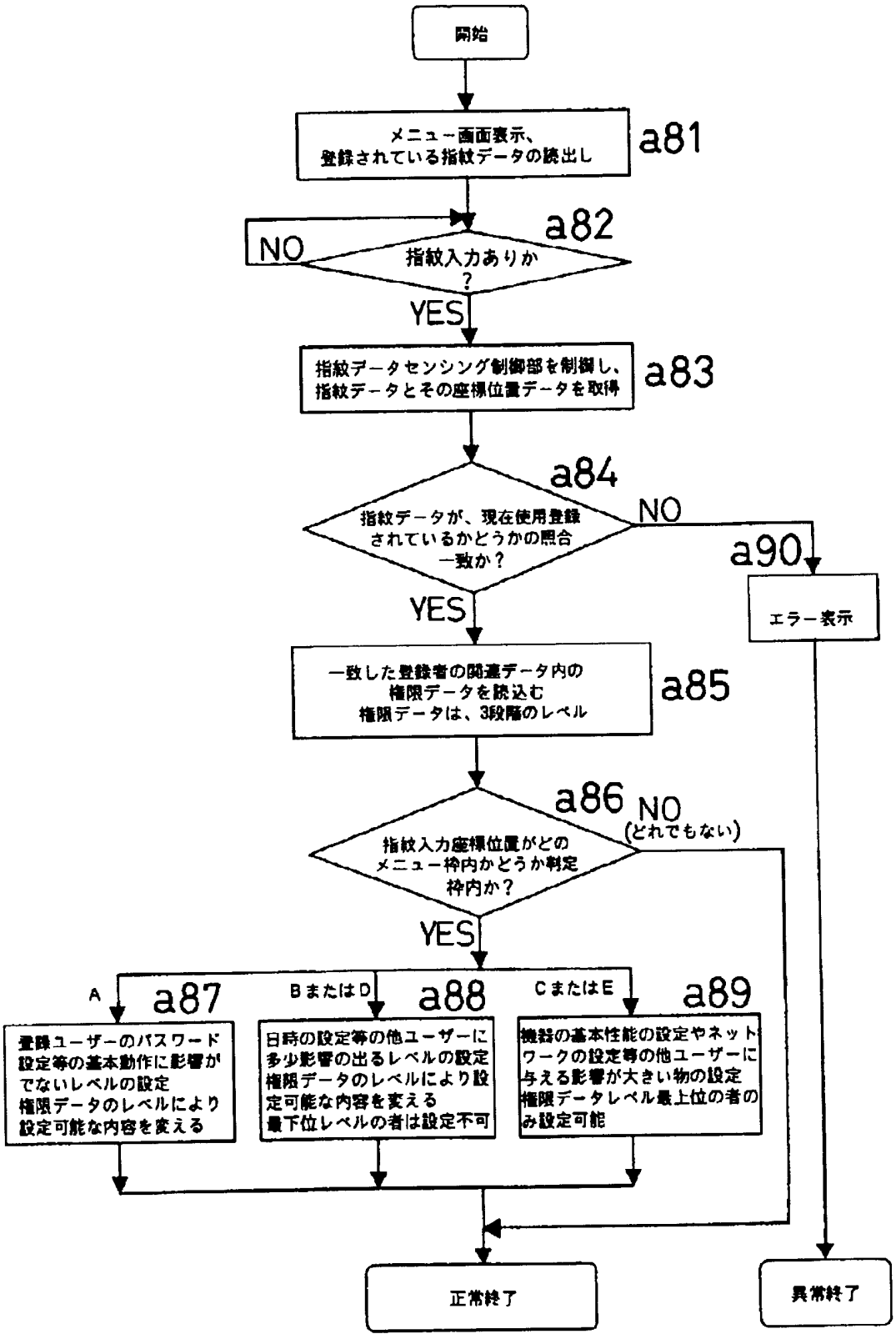
[Drawing 12]


開始
指紋入力表示、登録されている指紋データの読出し
a51
a52
NO
指紋入力ありか？
YES
指紋データセンシング制御部を制御し、指紋データとその座標位置データを取得
a53
a58
指紋データが、現在使用登録されているかどうかの照合一致か？
NO
エラー表示
a61
YES
a59
指紋データに関連データがあるか？
NO
YES
関連データにあるショートカット指定されているプログラム、ファイル等の起動
a60
正常終了
異常終了

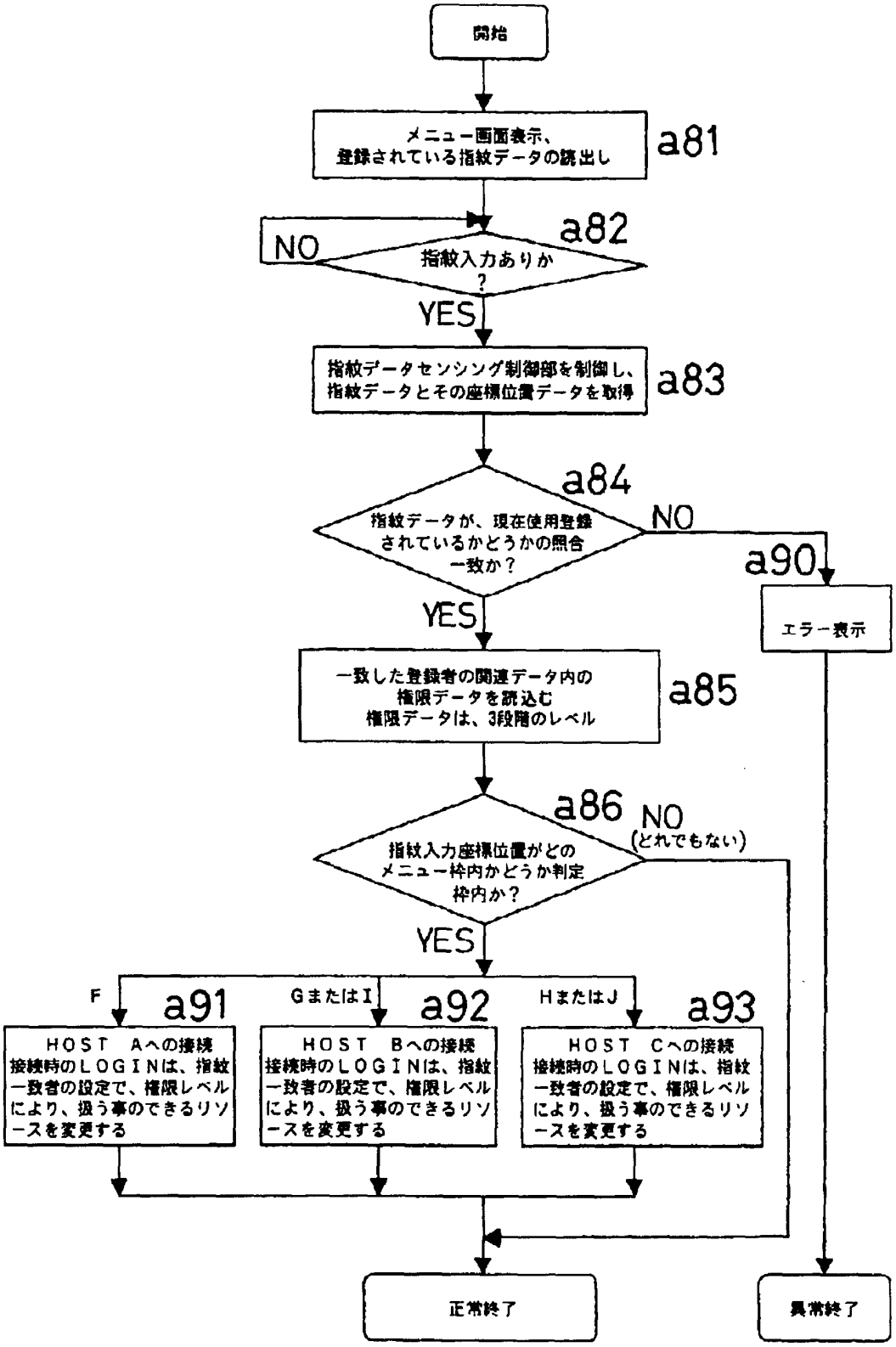
[Drawing 13]


開始
アプリケーションアイコン表示、登録されている指紋データの読出し
a71
NO
a72
指紋入力ありか？
YES
指紋データセンシング制御部を制御し、指紋データとその座標位置データを取得
a73
a74
指紋データが、現在使用登録されているかどうかの照合一致？
NO
a80
エラー表示
YES
a75
NO
(どれでもない)
指紋入力座標位置がどのアイコン枠内かどうか判定
枠内か？
YES
電話帳アイコン
スケジュールアイコン
ファイル関連アイコン
アプリケーションアイコン
a76
a77
a78
a79
指紋一致者に関連する電話帳データのみ表示、登録、変更、削除可能
指紋一致者に関連するスケジュールデータのみ表示、登録、変更、削除可能
指紋一致者に関連するファイルデータのみ表示、登録、変更、削除可能
指紋一致者が登録しているアプリケーションの起動を行う
正常終了
異常終了

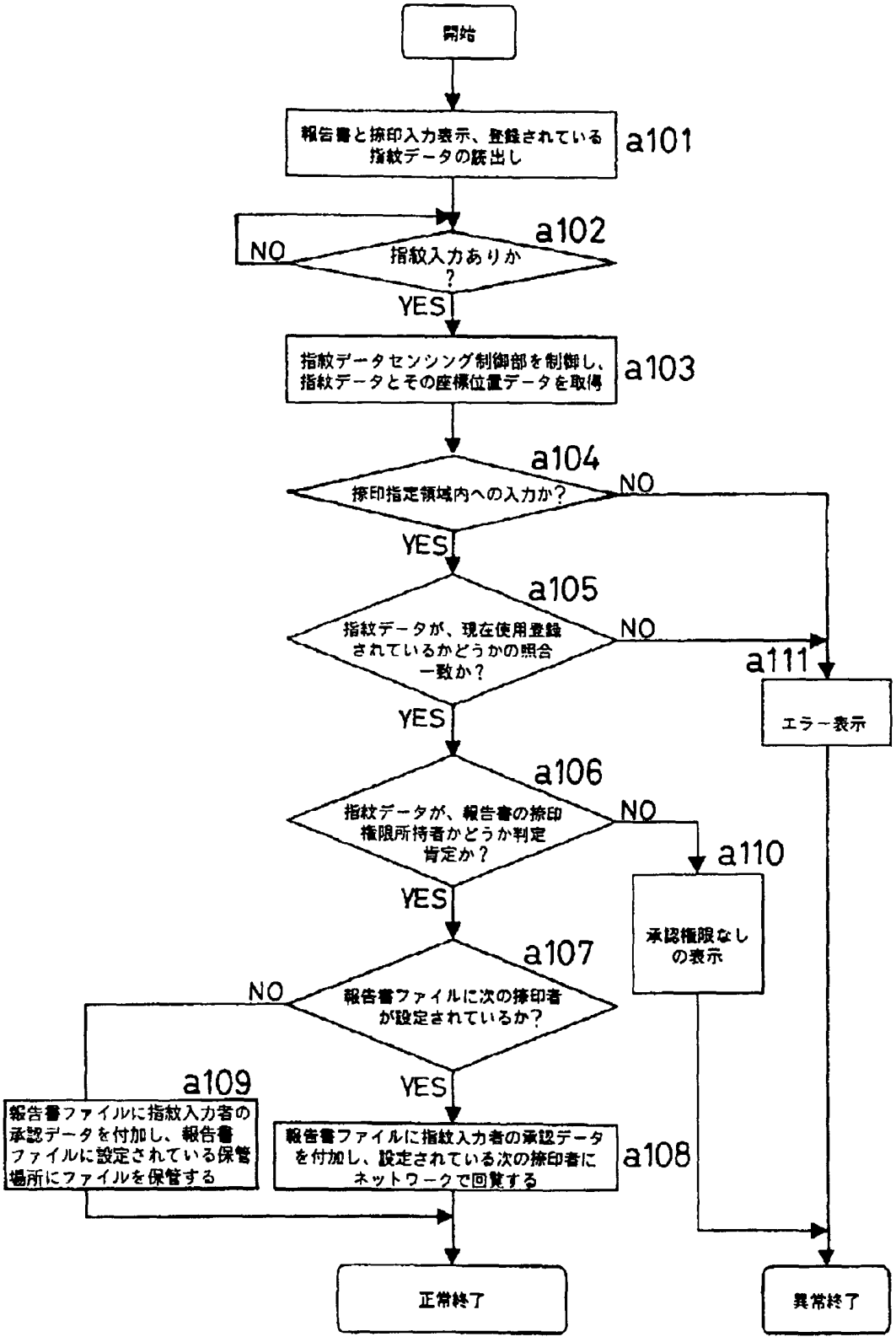
[Drawing 15]


開始
メニュー画面表示、
登録されている指紋データの読出し
a81
a82
NO
指紋入力ありか
?
YES
指紋データセンシング制御部を制御し、
指紋データとその座標位置データを取得
a83
a84
指紋データが、現在使用登録
されているかどうかの照合
一致か?
NO
a90
エラー表示
YES
一致した登録者の関連データ内の
権限データを読込む
権限データは、3段階のレベル
a85
a86
NO
(どれでもない)
指紋入力座標位置がどの
メニュー枠内かどうか判定
枠内か?
YES
A
a87
登録ユーザーのパスワード
設定等の基本動作に影響が
でないレベルの設定
権限データのレベルにより
設定可能な内容を変える
BまたはD
a88
日時の設定等の他ユーザーに
多少影響の出るレベルの設定
権限データのレベルにより設
定可能な内容を変える
最下位レベルの者は設定不可
CまたはE
a89
機器の基本性能の設定やネット
ワークの設定等の他ユーザーに
与える影響が大きい物の設定
権限データレベル最上位の者の
み設定可能
正常終了
異常終了

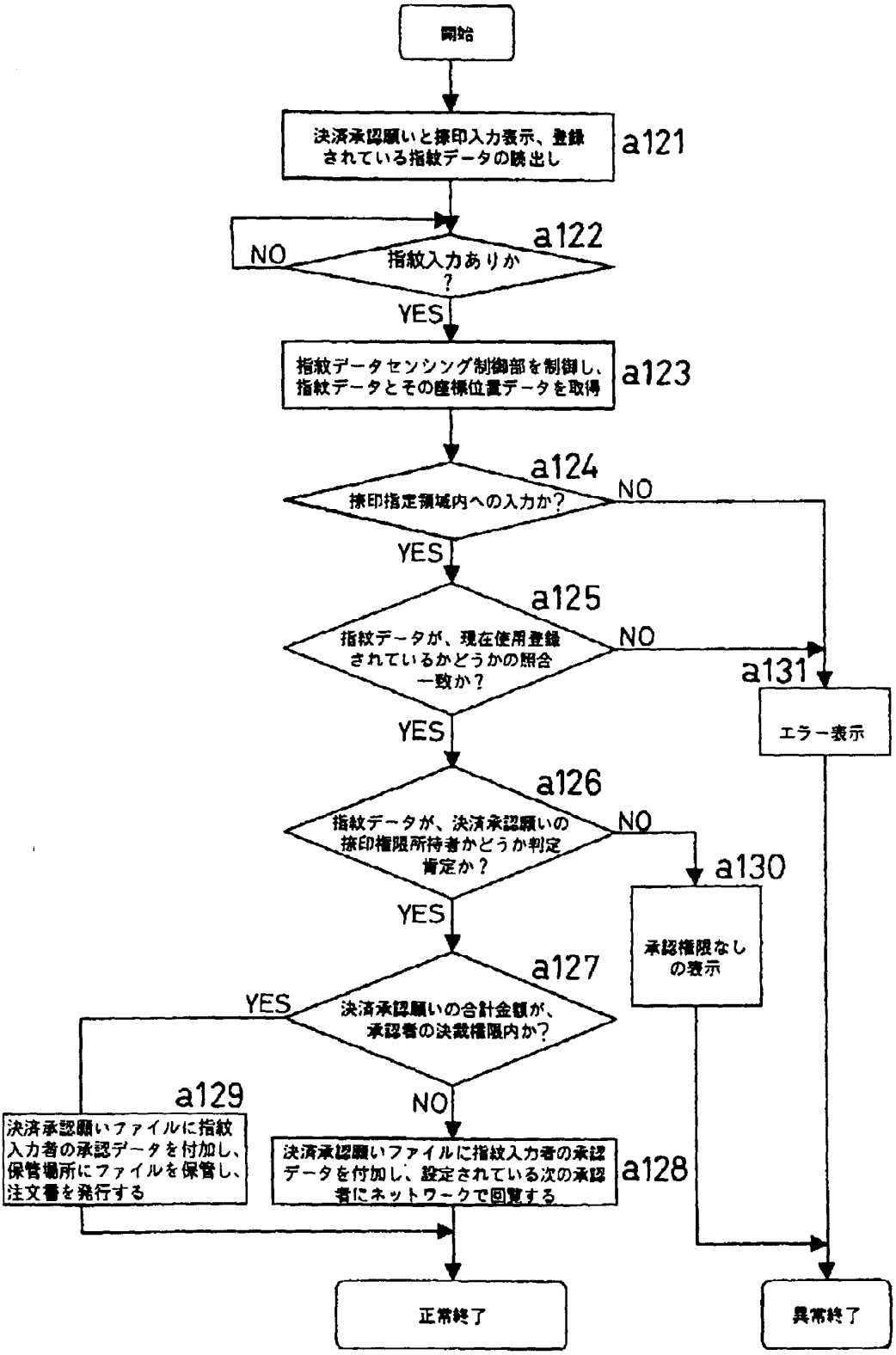
[Drawing 18]


開始
メニュー画面表示、
登録されている指紋データの読出し
a81
NO
a82
指紋入力ありか
?
YES
指紋データセンシング制御部を制御し、
指紋データとその座標位置データを取得
a83
a84
指紋データが、現在使用登録
されているかどうかの照合
一致か?
NO
a90
エラー表示
YES
一致した登録者の関連データ内の
権限データを読込む
権限データは、3段階のレベル
a85
a86
NO
(どれでもない)
指紋入力座標位置がどの
メニュー枠内かどうか判定
枠内か?
YES
F
a91
GまたはI
a92
HまたはJ
a93
HOST Aへの接続
接続時のLOGINは、指紋
一致者の設定で、権限レベル
により、扱う事のできるリソ
ースを変更する
HOST Bへの接続
接続時のLOGINは、指紋
一致者の設定で、権限レベル
により、扱う事のできるリソ
ースを変更する
HOST Cへの接続
接続時のLOGINは、指紋
一致者の設定で、権限レベル
により、扱う事のできるリソ
ースを変更する
正常終了
異常終了

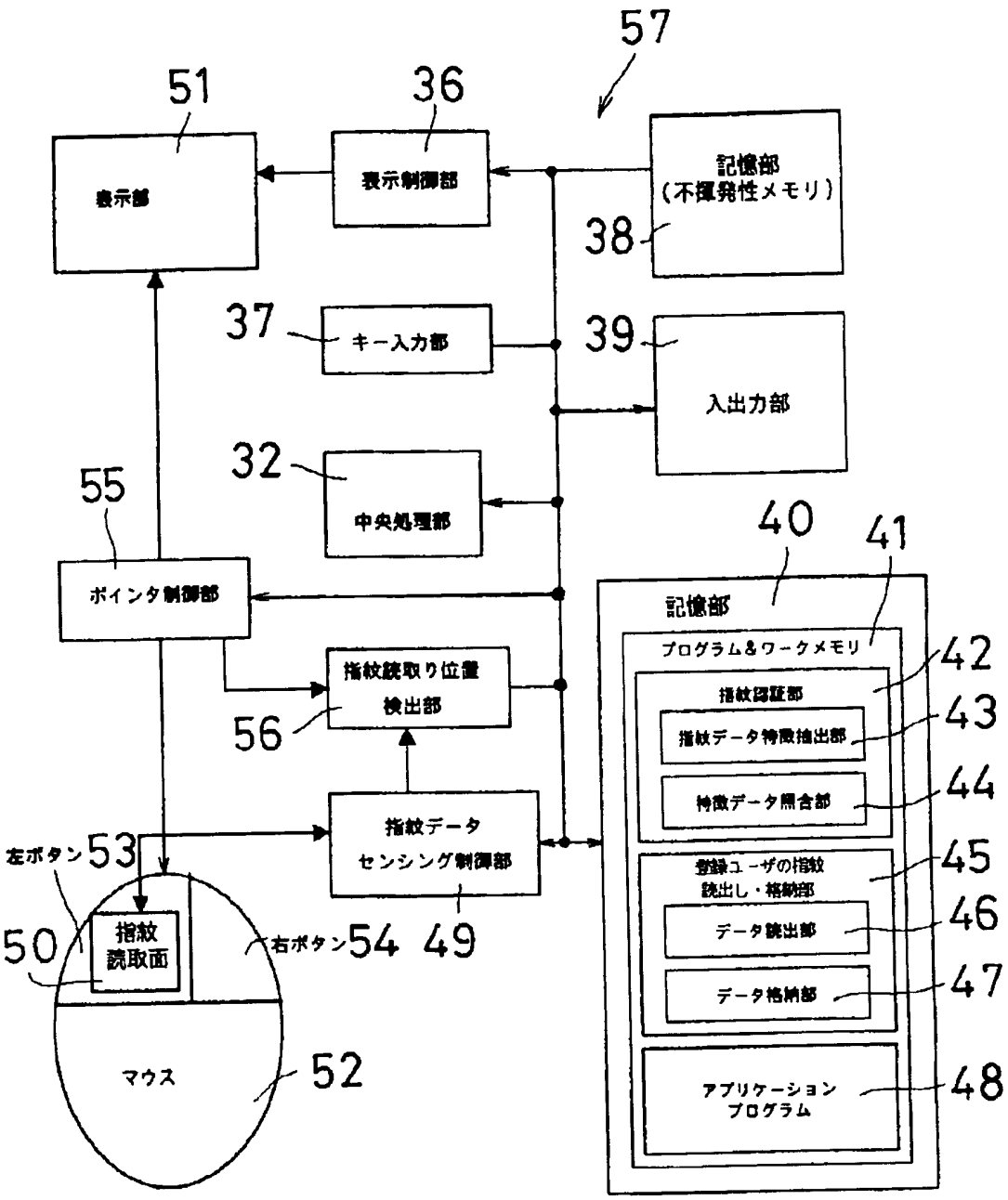
[Drawing 19]


開始
報告書と捺印入力表示、登録されている指紋データの読出し
a101
a102
NO
指紋入力ありか？
YES
指紋データセンシング制御部を制御し、指紋データとその座標位置データを取得
a103
a104
捺印指定領域内への入力か？
NO
YES
a105
指紋データが、現在使用登録されているかどうかの照合一致か？
NO
YES
a111
エラー表示
a106
指紋データが、報告書の捺印権限所持者かどうか判定肯定か？
NO
YES
a110
承認権限なしの表示
a107
報告書ファイルに次の捺印者が設定されているか？
NO
YES
a109
報告書ファイルに指紋入力者の承認データを付加し、報告書ファイルに設定されている保管場所にファイルを保管する
報告書ファイルに指紋入力者の承認データを付加し、設定されている次の捺印者にネットワークで回覧する
a108
正常終了
異常終了

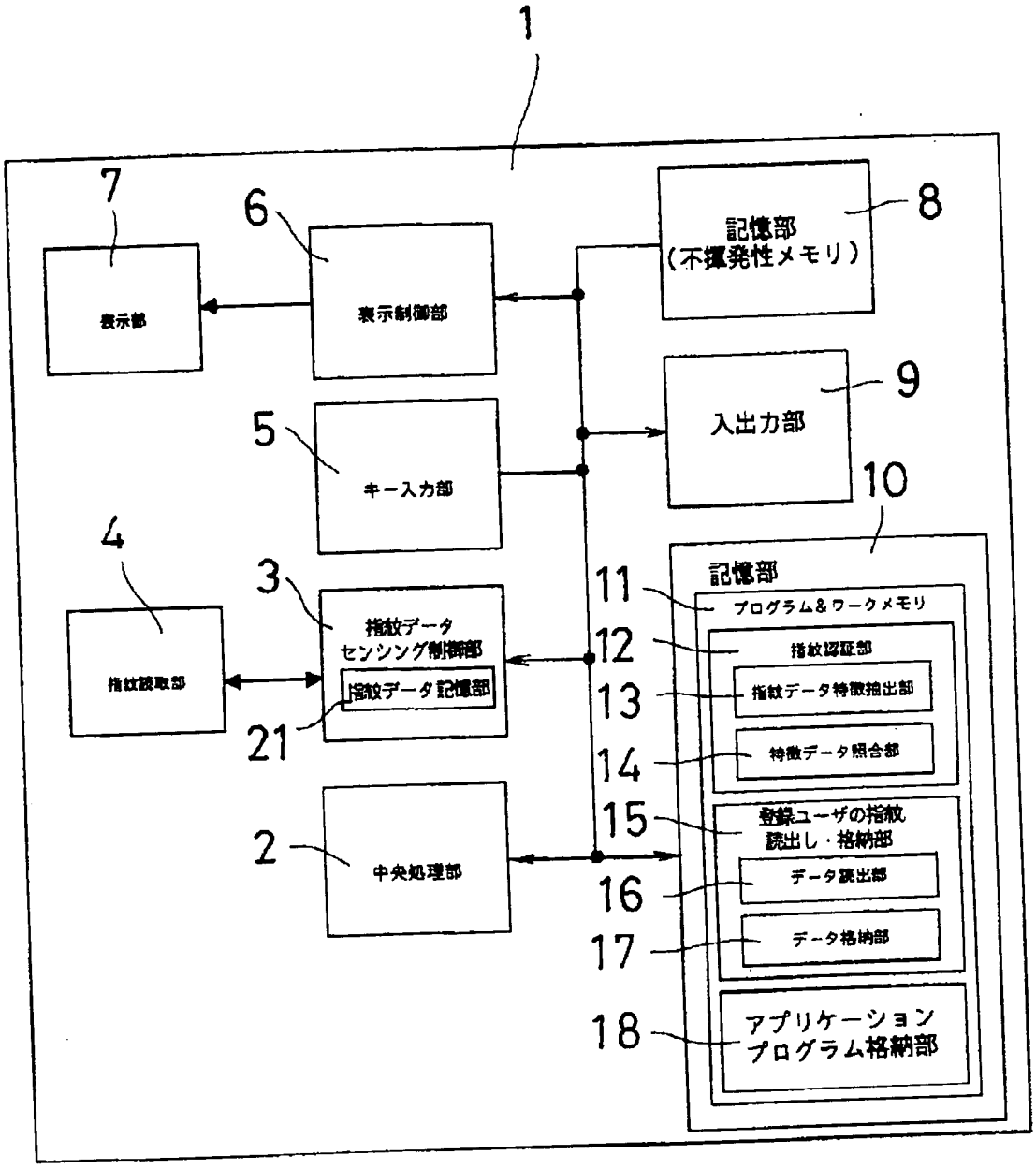
[Drawing 21]


開始
決済承認願いと捺印入力表示、登録されている指紋データの読出し
a121
a122
NO
指紋入力ありか？
YES
指紋データセンシング制御部を制御し、指紋データとその座標位置データを取得
a123
a124
捺印指定領域内への入力か？
NO
YES
a125
指紋データが、現在使用登録されているかどうかの照合一致か？
NO
YES
a131
エラー表示
a126
指紋データが、決済承認願いの捺印権限所持者かどうか判定肯定か？
NO
YES
a130
承認権限なしの表示
a127
決済承認願いの合計金額が、承認者の決裁権限内か？
YES
NO
a129
決済承認願いファイルに指紋入力者の承認データを付加し、保管場所にファイルを保管し、注文書を発行する
決済承認願いファイルに指紋入力者の承認データを付加し、設定されている次の承認者にネットワークで回覧する
a128
正常終了
異常終了

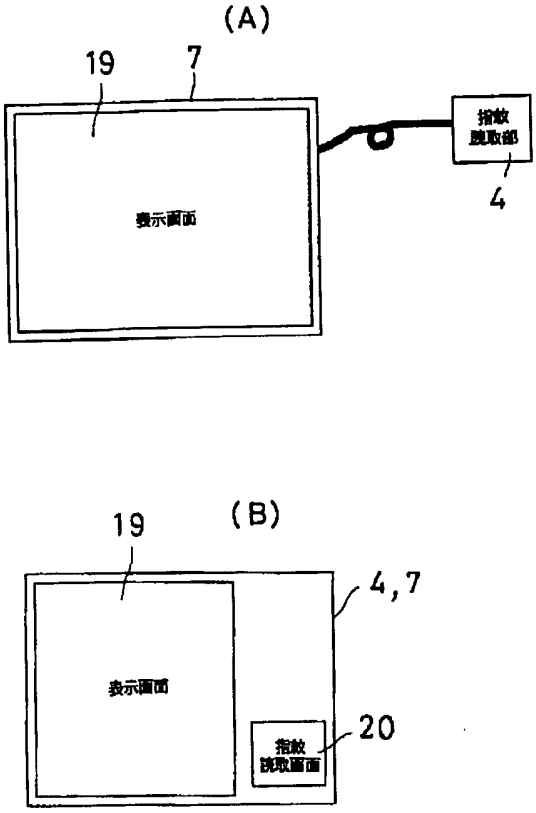
[Drawing 23]


57
51
36
表示部
表示制御部
記憶部
(不揮発性メモリ)
38
37
キー入力部
39
入出力部
32
中央処理部
55
40
41
ポインタ制御部
記憶部
プログラム&ワークメモリ
42
指紋認証部
指紋データ特徴抽出部
43
特徴データ照合部
44
指紋読取り位置
検出部
56
指紋データ
センシング制御部
登録ユーザの指紋
読出し・格納部
45
データ読出部
46
データ格納部
47
アプリケーション
プログラム
48
左ボタン53
50
指紋
読取面
右ボタン54
49
マウス
52

[Drawing 24]


1
7
表示部
6
表示制御部
記憶部
(不揮発性メモリ)
8
9
入出力部
5
キー入力部
10
記憶部
4
指紋読取部
3
指紋データ
センシング制御部
指紋データ記憶部
21
11
プログラム&ワークメモリ
12
指紋認証部
13
指紋データ特徴抽出部
14
特徴データ照合部
15
登録ユーザの指紋
読出し・格納部
2
中央処理部
16
データ読出部
17
データ格納部
18
アプリケーション
プログラム格納部

[Drawing 25]



[Translation done.]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－293253
（Ｐ2000－293253Ａ）
(43)公開日　平成12年10月20日(2000.10.20)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'（参考）
Ｇ０６Ｆ　1/00	３７０	Ｇ０６Ｆ	1/00	３７０Ｅ

審査請求　未請求　請求項の数16　ＯＬ　（全 29 頁）

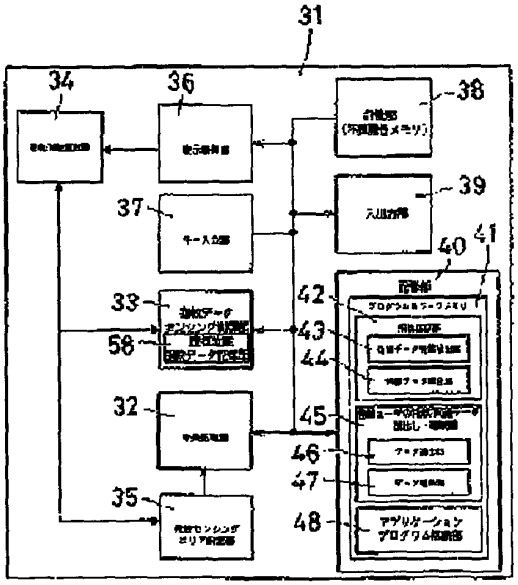
(21)出願番号　特願平11－98138

(22)出願日　平成11年４月５日(1999.4.5)

(71)出願人　000005049
シャープ株式会社
大阪府大阪市阿倍野区長池町22番22号
(72)発明者　樋上　貞彦
大阪府大阪市阿倍野区長池町22番22号　シャープ株式会社内
(72)発明者　原田　晃一
大阪府大阪市阿倍野区長池町22番22号　シャープ株式会社内
(74)代理人　100075557
弁理士　西教　圭一郎

(54)【発明の名称】　情報処理装置

(57)【要約】
【課題】　高いセキュリティ性および高い操作性を有する指紋認証機能を備える情報処理装置を提供する。
【解決手段】　表示・指紋読取部３４の指紋読取面から指紋が入力されると、指紋データセンシング制御部３３は指紋データおよび座標データを読取り、記憶部４０に格納する。指紋データは、予め登録されて記憶部３８に記憶された指紋データと照合され、一致する指紋があるかどうかの認証がなされる。情報処理装置３１では、このようにして指紋認証機能が実現される。また、指紋入力に関連する座標データに基づいて情報処理装置３１の動作が制御される。このように、指紋認証時における指の指紋読取面への接触による座標指定という簡単な操作によって情報処理装置３１の動作を制御することができる。



1

【特許請求の範囲】

【請求項１】　指紋読取面から読取った指紋を予め記憶された指紋と照合し認証する指紋認証手段を備える情報処理装置において、

直交座標が設定された表示面を有する表示手段と、

表示面上の指紋読取りに関連した座標を指定する座標指定手段と、

指定された座標に基づく動作制御を行う制御手段とを含むことを特徴とする情報処理装置。

【請求項２】　前記表示面と指紋読取面とが同一であることを特徴とする請求項１記載の情報処理装置。

【請求項３】　前記座標指定手段に指紋読取面が形成されていることを特徴とする請求項１記載の情報処理装置。

【請求項４】　前記制御手段は、特定座標が指定されたときに指紋認証手段を起動させることを特徴とする請求項１記載の情報処理装置。

【請求項５】　前記情報処理装置は、

指定された座標に基づく暗証番号を取得する暗証番号取得手段と、

取得された暗証番号を予め記憶された暗証番号と照合し認証する暗証番号認証手段と、をさらに含み、

前記制御手段は、暗証番号の認証結果に基づく動作制御を行うことを特徴とする請求項１記載の情報処理装置。

【請求項６】　前記制御手段は、暗証番号が一致していたときに指紋認証手段を起動させることを特徴とする請求項５記載の情報処理装置。

【請求項７】　前記制御手段は、指紋が一致していたときに情報処理装置の電源の動作を制御することを特徴とする請求項１記載の情報処理装置。

【請求項８】　前記制御手段は、指紋が一致していたときにユーザ毎に予め設定された動作条件の中から一致した指紋のユーザに対応する動作条件を読出して設定することを特徴とする請求項１記載の情報処理装置。

【請求項９】　前記指紋認証手段は各指の指紋認証が可能であることを特徴とする請求項１記載の情報処理装置。

【請求項１０】　前記制御手段は、各指の指紋が一致していたときにユーザの各指毎に予め登録されたコマンドの中から一致した指紋のユーザの各指に対応するコマンドを読出して実行することを特徴とする請求項９記載の情報処理装置。

【請求項１１】　前記情報処理装置は、

アプリケーションに対応したアイコンを設定するアイコン設定手段と、

指定された座標に基づいて設定されたアイコンが指定されたか否かを判定するアイコン指定判定手段と、をさらに含み、

前記制御手段は、アイコンが指定されかつ指紋が一致したとき、指定されたアイコンに対応するアプリケーションの一致した指紋のユーザのデータのみを読出して表示させることを特徴とする請求項１記載の情報処理装置。

2

【請求項１２】　前記制御手段は、アイコンが指定されかつ指紋が一致したとき、ユーザ毎に予め設定されたアプリケーションの中の一致した指紋のユーザに対応するアプリケーションを起動することを特徴とする請求項１１記載の情報処理装置。

【請求項１３】　前記アイコンにはユーザ毎のファイルが対応付けられており、

前記制御手段は、アイコンが指定されかつ指紋が一致したとき、前記ファイルの中の指定されたアイコンに対応するファイルの一致した指紋のユーザのファイルのみを開くことを特徴とする請求項１１記載の情報処理装置。

【請求項１４】　前記情報処理装置は、

メニューの実行レベルに対応した領域を設定するメニュー実行レベル領域設定手段と、

指定された座標に基づいて設定されたメニュー実行レベル領域が指定されたか否かを判定するメニュー実行レベル領域指定判定手段と、をさらに含み、

前記制御手段は、メニュー実行レベル領域が指定されかつ指紋が一致したとき、ユーザ毎に予め設定された実行レベルの中の一致した指紋のユーザに対応する実行レベルであって、指定されたメニュー実行レベル領域の実行レベルで、メニューを実行することを特徴とする請求項１記載の情報処理装置。

【請求項１５】　前記表示手段には、捺印欄を有する書類が表示され、

前記制御手段は、検出された座標が捺印欄の座標であったとき、前記書類の捺印欄に承認印を付加し、

前記情報処理装置はさらに、承認印が付加された書類を通信するための通信手段を含むことを特徴とする請求項１記載の情報処理装置。

【請求項１６】　前記表示手段には、捺印欄を有する書類が表示され、

前記制御手段は、検出された座標が捺印欄の座標であったとき、前記書類の捺印欄に承認印を付加し、

前記情報処理装置はさらに、承認印が付加された書類に対して付帯処理をする付帯処理手段を含むことを特徴とする請求項１記載の情報処理装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、指紋認証機能を備える情報処理装置に関する。

【０００２】

【従来の技術】ネットワーク社会の発展によって、情報処理装置とネットワークとの融合が進展し、個人認証などのセキュリティ機能の必要性が増してきている。個人認証としては、情報処理装置が他人に悪用されにくく、鍵やＩＣ（集積回路）カードのように紛失の可能性のない、指紋などの生体情報による認証が注目されている。

指紋の読取方式としてはプリズムなどの光学系を用いたものが主流であり、たとえば特開平８－３１５１４３号に開示されているが、液晶表示装置のＴＦＴ（薄膜トランジスタ）素子に隣接してフォトダイオードを配置してＣＣＤ（電荷結合素子）のようにして画像を読出す技術が特開平９－１８６３１２号に開示されている。また、指紋識別の手法に関する技術が特開平７－２２００７５号や特開平１０－１５４２３１号に開示されている。さらに、指紋認証結果に基づく情報処理装置の動作制御に関する技術が特開平１０－６９３２４号に開示されている。

【０００３】図２４は、指紋認証機能を備える従来技術の情報処理装置１のブロック図である。また図２５は、情報処理装置１の指紋読取部４と表示部７とを示す図である。情報処理装置１の中央処理部２には、指紋読取部４を制御する指紋データセンシング制御部３、キーボードなどのキー入力部５、液晶表示装置などの表示部７を制御する表示制御部６、不揮発性メモリで実現される記憶部８、ネットワークとの接続やプリンタなどの周辺機器との接続のための入出力部９および記憶部１０が接続され、装置全体の動作を統括的に制御する。

【０００４】記憶部８にはユーザの登録データが記憶されており、必要に応じて中央処理部２によって読出され、記憶部１０に転送され格納される。なお、アプリケーションプログラムも同様に記憶部８に記憶され、必要に応じて中央処理部２が読出し、記憶部１０に転送し格納されるが、記憶部１０に記憶しておいても構わない。

【０００５】指紋読取部４は、上述したような光学系を用いた特開平８－３１５１４３号の方式や特開平９－１８６３１２号の技術で実現される。指紋読取部４で読取られた指紋は、指紋データセンシング制御部３の指紋データ記憶部２１に一時記憶された後、記憶部１０に与えられる。

【０００６】記憶部１０は、指紋データの特徴抽出部１３と特徴データの照合部１４とを有する指紋認証部１２、データ読出部１６とデータ格納部１７とを有する登録ユーザの指紋読出し・格納部１５およびアプリケーションプログラム格納部１８で構成されるプログラム・ワークメモリ１１を備える。

【０００７】従来技術の情報処理装置１においては、図２５（Ａ）に示されるように指紋読取部４と表示部７の表示面１９とは独立して設けられる。またあるいは、図２５（Ｂ）に示されるように指紋読取部４の指紋読取面２０と表示部７の表示面１９とは独立して設けられる。このため、指紋読取りに関する座標を用いた情報処理装置１の動作制御は行われていない。

【０００８】

【発明が解決しようとする課題】本発明の目的は、高いセキュリティ性および高い操作性を有する指紋認証機能を備える情報処理装置を提供することである。

【０００９】

【課題を解決するための手段】本発明は、指紋読取面から読取った指紋を予め記憶された指紋と照合し認証する指紋認証手段を備える情報処理装置において、直交座標が設定された表示面を有する表示手段と、表示面上の指紋読取りに関連した座標を指定する座標指定手段と、指定された座標に基づく動作制御を行う制御手段とを含むことを特徴とする情報処理装置である。

【００１０】本発明に従えば、指紋読取面から読取られた指紋は予め記憶された指紋と照合され、一致する指紋があるかどうかの認証がなされる。情報処理装置では、このようにして指紋認証機能が実現される。また、指紋認証時には、表示手段の表示面上の指紋読取りに関連した座標が座標指定手段によって指定される。制御手段は、指定された座標に基づいて情報処理装置の動作を制御する。このように、指紋認証時における座標指定という簡単な操作によって情報処理装置の動作を制御することができる。

【００１１】また本発明は、前記表示面と指紋読取面とが同一であることを特徴とする。本発明に従えば、指紋認証時には指紋読取面である表示面にユーザの指が接触され、このようにして指紋読取面から読取られた指紋が照合され認証される。また、表示面上の指紋読取りに関連した座標、すなわち指を接触した位置の座標は、指の接触時に指定される。制御手段は、このような簡単な操作によって指定された座標に基づいて情報処理装置の動作を制御する。表示面と指紋読取面とが同一なので、指紋入力と座標指定とを同一の操作で行うことができ、高い操作性が得られる。

【００１２】また本発明は、前記座標指定手段に指紋読取面が形成されていることを特徴とする。

【００１３】本発明に従えば、指紋認証時には、座標指定手段に形成された指紋読取面にユーザの指が接触され、このようにして指紋読取面から読取られた指紋が照合され認証される。また、表示面上の指紋読取りに関連した座標は、座標指定手段によって指定される。制御手段は、このような簡単な操作によって指定された座標に基づいて情報処理装置の動作を制御する。座標指定手段に指紋読取面が形成されるので、座標指定と指紋入力とを同一の操作で行うことができ、高い操作性が得られる。

【００１４】また本発明は、前記制御手段は、特定座標が指定されたときに指紋認証手段を起動させることを特徴とする。

【００１５】本発明に従えば、指定された座標が特定の座標であったときに指紋認証手段を起動するよう情報処理装置の動作を制御することができる。したがって、特定座標以外の座標が指定されたときには指紋認証を行わないようにして、高いセキュリティ性を得ることができる。

5

【００１６】また本発明は、前記情報処理装置は、指定された座標に基づく暗証番号を取得する暗証番号取得手段と、取得された暗証番号を予め記憶された暗証番号と照合し認証する暗証番号認証手段と、をさらに含み、前記制御手段は、暗証番号の認証結果に基づく動作制御を行うことを特徴とする。

【００１７】本発明に従えば、指紋認証機能は上述したようにして実現される。また、表示手段の表示面上の指紋読取りに関連した座標が座標指定手段によって指定され、指定された座標に基づく暗証番号が暗証番号取得手段によって取得される。取得された暗証番号は予め記憶された暗証番号と照合され、一致しているかどうかの認証がなされる。情報処理装置ではまた、このようにして暗証番号の認証機能が実現される。制御手段は、暗証番号の認証結果に基づいて情報処理装置の動作を制御する。このように、指紋認証時における暗証番号を入力するための座標指定という簡単な操作によって情報処理装置の動作を制御することができる。

【００１８】また本発明は、前記制御手段は、暗証番号が一致していたときに指紋認証手段を起動させることを特徴とする。

【００１９】本発明に従えば、取得された暗証番号が予め記憶された暗証番号と一致していたときに指紋認証手段を起動するよう情報処理装置の動作を制御することができる。したがって、特定の暗証番号以外の番号が取得されたときには指紋認証を行わないようにして、高いセキュリティ性を得ることができる。

【００２０】また本発明は、前記制御手段は、指紋が一致していたときに情報処理装置の電源の動作を制御することを特徴とする。

【００２１】本発明に従えば、実行された指紋認証の結果、読取られた指紋が予め記憶された指紋と一致していたときに、情報処理装置の電源のオン／オフ動作が制御される。たとえば、指紋が一致していたときに、電源をオフ状態からオン状態にする。このようにして高いセキュリティ性および操作性を得ることができ、また消費電力の低減を図ることができる。

【００２２】また本発明は、前記制御手段は、指紋が一致していたときにユーザ毎に予め設定された動作条件の中から一致した指紋のユーザに対応する動作条件を読出して設定することを特徴とする。

【００２３】本発明に従えば、実行された指紋認証の結果、読取られた指紋が予め記憶された指紋と一致していたときに、ユーザ毎に予め設定された動作条件の中から一致した指紋のユーザに対応する動作条件が読出されて設定される。したがって、ユーザに適した操作環境や利用機能を設定することができ、高い操作性が得られる。

【００２４】また本発明は、前記指紋認証手段は各指の指紋認証が可能であることを特徴とする。

【００２５】本発明に従えば、前記指紋認証機能において各指の指紋認証が可能であるので、各指の指紋認証結果に基づく情報処理装置の細かな動作制御が可能となる。

6

【００２６】また本発明は、前記制御手段は、各指の指紋が一致していたときにユーザの各指毎に予め登録されたコマンドの中から一致した指紋のユーザの各指に対応するコマンドを読出して実行することを特徴とする。

【００２７】本発明に従えば、各指の指紋認証が可能な前記指紋認証機能において、各指の指紋が予め記憶された各指の指紋と一致していたときに、ユーザの各指毎に予め登録されたコマンドの中から一致した指紋のユーザの各指に対応するコマンドが読出されて実行される。このようにして高いセキュリティ性および操作性を得ることができ、また各指毎の細かな動作制御が可能となる。

【００２８】また本発明は、前記情報処理装置は、アプリケーションに対応したアイコンを設定するアイコン設定手段と、指定された座標に基づいて設定されたアイコンが指定されたか否かを判定するアイコン指定判定手段と、をさらに含み、前記制御手段は、アイコンが指定されかつ指紋が一致したとき、指定されたアイコンに対応するアプリケーションの一致した指紋のユーザのデータのみを読出して表示させることを特徴とする。

【００２９】本発明に従えば、指紋認証機能は上述したようにして実現される。また、表示手段の表示面上の指紋読取りに関連した座標が座標指定手段によって指定される。アイコン指定判定手段は、指定された座標に基づいて、アイコン設定手段によって設定されたアイコンが指定されたか否かを判定する。制御手段は、この判定結果および指紋認証結果に基づいて情報処理装置の動作を制御する。すなわち、アイコンが指定されかつ指紋が一致したとき、指定されたアイコンに対応するアプリケーションの一致した指紋のユーザのデータのみを読出して表示させる。このように、指紋認証時における座標指定という簡単な操作によって情報処理装置の動作を制御することができる。

【００３０】また本発明は、前記制御手段は、アイコンが指定されかつ指紋が一致したとき、ユーザ毎に予め設定されたアプリケーションの中の一致した指紋のユーザに対応するアプリケーションを起動することを特徴とする。

【００３１】本発明に従えば、制御手段は、アイコン指定の判定結果および指紋認証結果に基づいて情報処理装置の動作を制御する。すなわち、アイコンが指定されかつ指紋が一致したとき、ユーザ毎に予め設定されたアプリケーションの中の一致した指紋のユーザに対応するアプリケーションを起動する。このように、指紋認証時における座標指定という簡単な操作によって情報処理装置の動作を制御することができる。

【００３２】また本発明は、前記アイコンにはユーザ毎のファイルが対応付けられており、前記制御手段は、ア

イコンが指定されかつ指紋が一致したとき、前記ファイルの中の指定されたアイコンに対応するファイルの一致した指紋のユーザのファイルのみを開くことを特徴とする。

【００３３】本発明に従えば、制御手段は、アイコン指定の判定結果および指紋認証結果に基づいて情報処理装置の動作を制御する。すなわち、アイコンが指定されかつ指紋が一致したとき、ファイルの中の指定されたアイコンに対応するファイルの一致した指紋のユーザのファイルのみを開く。このように、指紋認証時における座標指定という簡単な操作によって情報処理装置の動作を制御することができる。

【００３４】また本発明は、前記情報処理装置は、メニューの実行レベルに対応した領域を設定するメニュー実行レベル領域設定手段と、指定された座標に基づいて設定されたメニュー実行レベル領域が指定されたか否かを判定するメニュー実行レベル領域指定判定手段と、をさらに含み、前記制御手段は、メニュー実行レベル領域が指定されかつ指紋が一致したとき、ユーザ毎に予め設定された実行レベルの中の一致した指紋のユーザに対応する実行レベルであって、指定されたメニュー実行レベル領域の実行レベルで、メニューを実行することを特徴とする。

【００３５】本発明に従えば、指紋認証機能は上述したようにして実現される。また、表示手段の表示画上の指紋読取りに関連した座標が座標指定手段によって指定される。メニュー実行レベル領域指定判定手段は、指定された座標に基づいて、メニュー実行レベル領域設定手段によって設定されたメニュー実行レベル領域が指定されたか否かを判定する。制御手段は、この判定結果および指紋認証結果に基づいて情報処理装置の動作を制御する。すなわち、メニュー実行レベル領域が指定されかつ指紋が一致したとき、ユーザ毎に予め設定された実行レベルの中の一致した指紋のユーザに対応する実行レベルであって、指定されたメニュー実行レベル領域の実行レベルでメニューを実行する。このように、指紋認証時における座標指定という簡単な操作によって情報処理装置の動作を制御することができる。

【００３６】また本発明は、前記表示手段には、捺印欄を有する書類が表示され、前記制御手段は、検出された座標が捺印欄の座標であったとき、前記書類の捺印欄に承認印を付加し、前記情報処理装置はさらに、承認印が付加された書類を通信するための通信手段を含むことを特徴とする。

【００３７】本発明に従えば、捺印欄を有する書類に対して、指紋読取りに関連して指定された座標が捺印欄内の座標であったときには、承認印が付加される。さらに、承認印が付加された書類は通信手段によって通信される。したがって、報告書などの書類を次の人に転送して回覧することができる。

【００３８】また本発明は、前記表示手段には、捺印欄を有する書類が表示され、前記制御手段は、検出された座標が捺印欄の座標であったとき、前記書類の捺印欄に承認印を付加し、前記情報処理装置はさらに、承認印が付加された書類に対して付帯処理をする付帯処理手段を含むことを特徴とする。

【００３９】本発明に従えば、捺印欄を有する書類に対して、指紋読取りに関連して指定された座標が前記捺印欄内の座標であったときには、承認印が付加される。さらに、承認印が付加された書類は付帯処理手段によって付帯手段される。したがって、決済承認願などの書類に対して注文書の発行処理を行うことができる。

【００４０】

【発明の実施の形態】図１は、本発明の実施の一形態である情報処理装置３１のブロック図である。指紋認証機能を備える情報処理装置３１の中央処理部３２には、表示・指紋読取部３４の指紋読取動作を制御する指紋データセンシング制御部３３、指紋センシングエリア設定部３５、表示・指紋読取部３４の表示動作を制御する表示制御部３６、キーボードなどのキー入力部３７、不揮発性メモリで実現される記憶部３８、ネットワークとの接続やプリンタなどの周辺機器との接続のための入出力部３９および記憶部４０が接続され、装置全体の動作を統括的に制御する。

【００４１】表示・指紋読取部３４において、たとえば液晶表示装置で実現される表示部の直交座標が設定された表示面と、公知の技術によって実現される指紋読取部の指が接触される指紋読取面とは同一である。具体的には、液晶表示装置のすべての画素にデータ読取りのためのセンサが設けられる。該センサは液晶表示装置のすべての画素に設ける必要はなく、一部の画素だけに設けても構わない。このようにして、図２に示される表示・データ読取画面５９を有する表示・指紋読取部３４によって、画面５９の上の座標データと指紋データとが取得される。中央処理部３２は、取得された座標データに基づいて情報処理装置３１の動作を制御し、また取得された指紋データに基づいて装置３１の動作を制御する。

【００４２】なお、表示・指紋読取部３４として、たとえば本願出願人による特願平１１－１２２３１号に記載した画像読取装置であって、液晶層内部に受光素子を埋込んで指紋データを読取る画像読取装置を採用しても構わない。情報処理装置３１では、指紋読取手段、表示手段および座標指定手段が表示・指紋読取部３４によって実現される。

【００４３】指紋データセンシング制御部３３の座標位置・指紋データ記憶部５８には、表示・指紋読取部３４で取得された座標データと指紋データとが一時記憶される。これらの記憶データは記憶部４０に転送される。表示・指紋読取部３４には、表示制御部３６から表示データが与えられる。また、表示・指紋読取部３４の表示動

作と指紋読取動作とのタイミングの制御は、中央処理部３２によって行われる。

【００４４】指紋センシングエリア設定部３５は、画面５９中に指紋読取領域６０を設定する。該領域６０は、たとえば入力ペンなどの指示手段によって指定された２点の座標を向かい合った頂点とする矩形領域である。キー入力部３７からは、必要に応じて指紋データに対する付加データなどが入力される。

【００４５】記憶部３８には予め登録されたユーザ登録データが記憶されており、必要に応じて中央処理部３２によって読出され、記憶部４０に転送され格納される。なお、アプリケーションプログラムも同様に記憶部３８に記憶され、必要に応じて中央処理部３２が読出し、記憶部４０に転送し格納されるが、記憶部４０に記憶しておいても構わない。

【００４６】記憶部４０は、指紋認証部４２、ユーザの登録データの読出し・格納部４５およびアプリケーションプログラム格納部４８で構成されるプログラム・ワークメモリ４１を備える。指紋認証部４２は、指紋データの特徴データを抽出する特徴抽出部４３と、抽出された特徴データを照合する照合部４４とを有する。ユーザの登録データの読出し・格納部４５は、ユーザ登録データを読出すデータ読出部４６と、読出されたユーザ登録データを格納するデータ格納部４７とを有する。

【００４７】図３は、記憶部３８のユーザ登録データを示す図である。ユーザ登録データは、ユーザ毎の、基本データ部６１と関連データ部６２とで構成される。基本データ部６１は、ユーザの氏名データ格納部６３、指紋データの格納部６４および後継・代理決済者データの格納部６５で構成される。前記指紋データの格納部６４には、左手各指の指紋データ６４ａと右手各指の指紋データ６４ｂとがそれぞれ格納される。関連データ部６２は、操作環境データの格納部６６、利用機能の制限データの格納部６７、各指のショートカットデータの格納部６８、権限データの格納部６９および起動アプリケーションの設定データの格納部７０で構成される。前記権限データの格納部６９には、機器設定変更レベル６９ａ、ネットワーク接続変更レベル６９ｂおよびその他のデータ６９ｃがそれぞれ格納される。

【００４８】操作環境とは情報処理装置３１の動作条件に相当し、たとえば操作案内を行うヘルプ情報などの特定情報の表示／非表示、スクリーンキーなどの特定キーのオン／オフ、表示される文字の大きさなどを規定するデータである。利用機能の制限データも動作条件に相当し、たとえば接続されるＣＤ（コンパクトディスク）－ＲＯＭ（リードオンリメモリ）からのデータ読出しの可／不可、ＳＩＯ（ファイル転送プロトコル）の利用の可／不可などを規定するデータである。各指のショートカットデータはユーザの各指毎に予め設定されたコマンドに相当し、たとえばスケジュールの登録機能の実行を指定するコマンドである。権限データとは、機器設定変更レベルやネットワーク接続変更レベルなどを規定するデータである。起動アプリケーションとは、決済承認願に捺印されたときに実行される注文書発行のアプリケーションや報告書に捺印されたときに実行されるネットワーク接続のアプリケーションである。

【００４９】図４は、情報処理装置３１の第１動作を示すフローチャートである。ステップａ１では、指紋の読取りに必要な要素、すなわち中央処理部３２、指紋データセンシング制御部３３および表示・指紋読取部３４を電源オン状態とし、指紋の読取りに必要でない要素は電源オフ状態として、比較的遅い指紋入力の検出周期で指紋入力を待つ。指紋の入力があるまでこの状態が維持され、このようにして消費電力の低減が図られる。

【００５０】次のステップａ２では、表示・指紋読取部３４の表示・データ読取画面５９への指の接触による電源オンの操作があったか否かを中央処理部３２が判断する。指が接触されて、電源オン操作があったと判断すると、次のステップａ３に進む。指が接触されると、指紋データセンシング制御部３３は中央処理部３２に対して割込信号を発生する。この割込信号に基づいて中央処理部３２は電源オンの操作ありの判断を行う。またあるいは、中央処理部３２から指紋データセンシング処理部３３へのポーリングによるステータスの読出しによって、中央処理部３２は電源オンの操作ありの判断を行う。

【００５１】ステップａ３では、情報処理装置３１全体の電源状態をオンとし、指紋データセンシング制御部３３は表示・指紋読取部３４から指紋データと指が接触された位置の座標データとを読出し、記憶部５８に一時記憶する。これらのデータは、中央処理部３２を介して記憶部４０に転送される。またあるいは、中央処理部３２を介さずにＤＭＡ（ダイレクトメモリアクセス）によってそのまま記憶部４０に転送される。

【００５２】次のステップａ４では、取得された座標データによる位置が特定の位置であるか否かを中央処理部３２が判断する。特定位置であったときにはステップａ５に進み、特定位置でなかったときにはステップａ２に戻る。

【００５３】ステップａ５では、中央処理部３２は、記憶部３８に登録されているユーザ登録データの指紋データを読出し、記憶部４０に格納する。次のステップａ６では、中央処理部３２は取得された指紋データと記憶部３８から読出された指紋データとを、記憶部４０に記憶された指紋認証プログラムによって照合し認証する。次のステップａ７では、指紋が一致しているか否かを判断する。一致しているときには電源オン状態を維持して動作を終了する。一致していないときにはステップａ８に進む。

【００５４】ステップａ８では、記憶部３８に登録されている指紋データがまだあるか否かを判断し、まだある

ときにはステップａ５に戻って登録されている指紋データがなくなるまで指紋認証動作を繰返す。登録されている指紋データがもうないときにはステップａ９に進み、エラー表示を行ってステップａ１に戻る。

【００５５】なお、記憶部４０に記憶された指紋認証プログラムは、記憶部３８から読出されて格納されたものである。該プログラムは指紋認証の度に読出して格納する必要はなく、最初に読出して格納したプログラムを繰返し使用しても構わない。

【００５６】また、ここでは、記憶部３８に登録されている指紋データを認証の度に記憶部４０に読出す例について説明したが、登録されているすべての指紋データを最初に読出すようにしても構わない。

【００５７】さらに、ステップａ９のエラー表示は必要に応じて行えばよく、ステップａ８で登録されている指紋データがもうないときには直ちにステップａ１に進んでも構わない。

【００５８】図５は、情報処理装置３１の第２動作を示すフローチャートである。このフローチャートは図４のフローチャートにステップａ１０、ａ１１を追加したものであり、同じステップの説明は省略する。ステップａ７で指紋が一致しているか否かを判断し、一致していたときにはステップａ１０に進む。ステップａ１０では、記憶部３８に登録されている関連データのうち、一致した指紋のユーザに対応した関連データがあるか否かを判断する。あるときにはステップａ１１に進んで該関連データを読出す。そして、該関連データに基づいた操作環境や利用機能を設定して、電源オン状態を維持して動作を終了する。関連データがないときにはそのままの電源オン状態を維持して動作を終了する。

【００５９】図６は、情報処理装置３１の第３動作を示すフローチャートである。ステップａ２１では、表示・指紋読取部３４の表示・データ読取画面５９に図７に示されるような暗証番号の入力を促す画面７１が設定され表示される。画面７１には、０～９までの数値を指定して暗証番号を入力するための暗証番号入力領域７２が設定されている。なお、該領域７２は指紋入力領域でもある。次のステップａ２２では、画面７１の暗証番号入力領域７２への指の接触による暗証番号の入力操作があったか否かを中央処理部３２が判断する。領域７２に指が接触されて、暗証番号の入力操作があったと判断すると、次のステップａ２３に進む。ここで、暗証番号の入力と同時に指紋も入力される。また、領域７２以外の領域への指の接触は無視される。

【００６０】ステップａ２３では、指紋データセンシング制御部３３は表示・指紋読取部３４から指紋データと指が接触された位置の座標データとを読出し、記憶部５８に一時記憶する。次のステップａ２４では、取得された座標データによる位置に基づいて、暗証番号を検知し取得する。次のステップａ２５では、取得された指紋データを記憶部４０に格納する。次のステップａ２６では、暗証番号の入力が予め定められた桁数、たとえば４桁まで行われたか否かを判断する。入力されたときにはステップａ２７に進み、入力されていないときにはステップａ２２に戻る。

【００６１】ステップａ２７では、中央処理部３２は、取得された暗証番号と予め登録された暗証番号とを照合し認証して、両者が一致しているか否かを判断する。一致しているときにはステップａ２８に進み、一致していないときにはステップａ２９に進む。暗証番号が一致していたステップａ２８では、中央処理部３２は、取得された指紋データと予め記憶された指紋データとを照合し認証して、両者が一致しているか否かを判断する。一致しているときにはそのまま動作を終了し、一致していないときにはステップａ３０に進む。ステップａ２９，ａ３０では、エラー表示を行って動作を終了する。

【００６２】なお、暗証番号の認証プログラムは前記指紋認証プログラムと同様に、記憶部３８から読出されて記憶部４０に格納される。該プログラムも暗証番号の認証の度に読出して格納する必要はなく、最初に読出して格納したプログラムを繰返し使用しても構わない。また、ステップａ２９，ａ３０のエラー表示は必要に応じて行えばよく、ステップａ２７，２８の動作終了後、直ちに動作を終了しても構わない。

【００６３】図８は、情報処理装置３１の第４動作を示すフローチャートである。ステップａ４１では、表示・指紋読取部３４の表示・データ読取画面５９に図９に示されるような指紋の入力を促す画面７３が設定され表示される。画面７３には、複数の指紋入力枠７４が設定されている。また、記憶部３８に記憶された指紋データが読出され記憶部４０に格納される。

【００６４】次のステップａ４２では、画面７３の指紋入力枠７４内への指の接触による指紋の入力操作があったか否かを中央処理部３２が判断する。枠７４内に指が接触されて、指紋の入力操作があったと判断すると、次のステップａ４３に進む。ここで、枠７４外への指の接触は無視される。

【００６５】ステップａ４３では、指紋データセンシング制御部３３は表示・指紋読取部３４から指紋データと指が接触された位置の座標データとを読出し、記憶部５８に一時記憶する。次のステップａ４４では、取得された座標データによる位置に基づいて、入力された枠７４を検知して取得する。次のステップａ４５では、取得された指紋データを記憶部４０に格納する。次のステップａ４６では、指紋入力があった枠順と、予め登録された枠順とを照合し認証して、両者が一致しているか否かを判断する。一致しているときにはステップａ４７に進み、一致していないときにはステップａ４８に進む。

【００６６】ステップａ４７では、中央処理部３２は、予め登録された枠順をすべて照合し認証したか否かを判

断する。すべて照合し認証したときにはそのまま動作を終了し、すべて照合し認証していないときにはステップａ４２に戻る。ステップａ４８では、エラー表示を行って動作を終了する。

【００６７】なお、枠順の認証プログラムは前記指紋認証プログラムと同様に、記憶部３８から読出されて記憶部４０に格納される。該プログラムも枠順の認証の度に読出して格納する必要はなく、最初に読出して格納したプログラムを繰返し使用しても構わない。また、ステップａ４８のエラー表示は必要に応じて行えばよく、ステップａ４６で枠順が一致していなかったときには直ちに動作を終了しても構わない。

【００６８】図１０は、情報処理装置３１の第５動作を示すフローチャートである。ステップａ５１では、表示・指紋読取部３４の表示・データ読取画面５９に図１１に示されるような指紋の入力を促す画面７５が設定され表示される。画面７５には、各指毎の指紋入力枠７６が設定されている。また、記憶部３８に記憶された指紋データが読出され記憶部４０に格納される。

【００６９】次のステップａ５２では、画面７５の指紋入力枠７６内への指の接触による指紋の入力操作があったか否かを中央処理部３２が判断する。枠７６内に指が接触されて、指紋の入力操作があったと判断すると、次のステップａ５３に進む。ここで、枠７６外への指の接触は無視される。

【００７０】ステップａ５３では、指紋データセンシング制御部３３は表示・指紋読取部３４から指紋データと指が接触された位置の座標データとを読出し、記憶部５８に一時記憶する。次のステップａ５４では、取得された座標データによる位置に基づいて、入力された枠７６を検知して取得し、どの指の指紋データであるかのラベリングを行う。次のステップａ５５では、取得されたラベリングされた各指紋データを記憶部４０に格納する。

【００７１】次のステップａ５６では、ラベリングされた各指紋データと、予め登録された指紋データとを照合し認証して、両者が一致しているか否かを判断する。また、指紋入力があった枠順と、予め登録された枠順とを照合し認証して、両者が一致しているか否かを判断する。ここで、指紋および枠順は、その両方を判断してもよいし、いずれか一方を判断しても構わない。指紋および／または枠順が一致しているときにはそのまま動作を終了し、一致していないときにはステップａ５７に進んでエラー表示を行って動作を終了する。

【００７２】なお、ステップａ５７のエラー表示は必要に応じて行えばよく、ステップａ５６で指紋および／または枠順が一致していないときには直ちに動作を終了しても構わない。

【００７３】図１２は、情報処理装置３１の第６動作を示すフローチャートである。このフローチャートは、図１０のフローチャートのステップａ５４～ａ５７を削除し、ステップａ５８～ａ６１を追加したものであり、同じステップの説明は省略する。ステップａ５３で、指紋データセンシング制御部３３は表示・指紋読取部３４から指紋データと指が接触された位置の座標データとを読出し、記憶部５８に一時記憶し、記憶部４０に転送すると、次のステップａ５８では、指紋データを照合し認証して、一致しているか否かを判断する。一致しているときにはステップａ５９に進み、一致していないときにはステップａ６１に進む。

【００７４】ステップａ５９では、一致していた指紋データのユーザに対応する関連データが記憶されているか否かを判断する。記憶されているときにはステップａ６０に進み、関連データによる各指毎に予め設定されたコマンドを読出して実行して動作を終了する。関連データが記憶されていないときにはそのまま動作を終了する。ステップａ６１では、エラー表示を行って動作を終了する。

【００７５】なお、ステップａ６１のエラー表示は必要に応じて行えばよく、ステップａ５８で指紋データが一致していないときには直ちに動作を終了しても構わない。

【００７６】図１３は、情報処理装置３１の第７動作を示すフローチャートである。ステップａ７１では、表示・指紋読取部３４の表示・データ読取画面５９に図１４に示されるようなアイコンの指定を促す画面７７が設定され表示される。画面７７には、複数のアイコン７８ａ～７８ｆが設定されている。なお、該アイコン７８ａ～７８ｆの領域は指紋入力領域でもある。また、記憶部３８に記憶された指紋データが読出され記憶部４０に格納される。

【００７７】次のステップａ７２では、画面７７への指の接触による指紋の入力操作があったか否かを中央処理部３２が判断する。指が接触されて、指紋の入力操作があったと判断すると、次のステップａ７３に進む。ここで、アイコン７８ａ～７８ｆ外への指の接触によって、次の処理に進まないよう制御することも可能である。

【００７８】ステップａ７３では、指紋データセンシング制御部３３は表示・指紋読取部３４から指紋データと指が接触された位置の座標データとを読出し、記憶部５８に一時記憶し、記憶部４０に転送する。次のステップａ７４では、指紋データを照合し認証して、一致しているか否かを判断する。一致しているときにはステップａ７５に進み、一致していないときにはステップａ８０に進んで、エラー表示を行って動作を終了する。

【００７９】ステップａ７５では、指紋入力がどのアイコン７８ａ～７８ｆ内になされたかを判断する。電話帳アイコン７８ａのときにはステップａ７６に、スケジュールアイコン７８ｂのときにはステップａ７７に、ファイル管理アイコン７８ｃのときにはステップａ７８に、アプリケーションアイコン７８ｄのときにはステップａ

７９にそれぞれ進む。このフローチャートにはないが、アイコン７８ｅのときは手書きメモのアプリケーションを、アイコン７８ｆのときには音声メモのアプリケーションを起動し、終了する。アイコン７８ａ～７８ｆ外のときにはそのまま動作を終了する。ステップａ７６～ａ７８では、指定された各アイコン７８ａ～７８ｃに対応するアプリケーションの、一致した指紋のユーザのデータのみを読出して表示し、登録、変更および削除などのデータ編集を可能として、動作を終了する。また、ステップａ７９では、ユーザ毎に予め登録されたアプリケーションの中の、一致した指紋のユーザに対応するアプリケーションを起動して、動作を終了する。

【００８０】なお、ステップａ８０のエラー表示は必要に応じて行えばよく、ステップａ７４で指紋データが一致しないときには直ちに動作を終了しても構わない。

【００８１】図１５は、情報処理装置３１の第８動作を示すフローチャートである。ステップａ８１では、表示・指紋読取部３４の表示・データ読取画面５９に図１６に示されるようなメニューの指定を促す画面７９が設定され表示される。ここで、メニューはマシン設定およびネットワーク接続の２つであり、前記画面７９には２つのメニュー指定領域８０ａ，８０ｂが設定されている。なお、該メニュー指定領域８０ａ，８０ｂは指紋入力領域でもある。また、記憶部３８に記憶された指紋データが読出され記憶部４０に格納される。

【００８２】メニュー指定を促す前記画面７９のメニュー指定領域８０ａ，８０ｂは、具体的に図１７に示されるように複数の領域Ａ～Ｊに区分されている。領域８０ａ，８０ｂの中のどの領域Ａ～Ｊに指紋入力がなされたかによって、メニュー実行時の権限レベルが指定される。

【００８３】次のステップａ８２では、画面７９への指の接触による指紋の入力操作があったか否かを中央処理部３２が判断する。指が接触されて、指紋の入力操作があったと判断すると、次のステップａ８３に進む。ここで、メニュー指定領域８０ａ，８０ｂ外への指の接触によって、次の処理に進まないよう制御することも可能である。

【００８４】ステップａ８３では、指紋データセンシング制御部３３は表示・指紋読取部３４から指紋データと指が接触された位置の座標データとを読出し、記憶部５８に一時記憶し、記憶部４０に転送する。次のステップａ８４では、指紋データを照合し認証して、一致しているか否かを判断する。一致しているときにはステップａ８５に進み、一致していないときにはステップａ９０に進んで、エラー表示を行って動作を終了する。

【００８５】ステップａ８５では、一致した指紋のユーザに対応する権限データを記憶部３８から読出し、記憶部４０に格納する。次のステップａ８６では、指紋入力がどの領域Ａ～Ｅ内になされたかを判断する。領域Ａのときにはステップａ８７に、領域ＢまたはＤのときにはステップａ８８に、領域ＣまたはＥのときにはステップａ８９にそれぞれ進み、読出され格納された権限データのレベルであって、各領域Ａ～Ｅで指定される権限レベルでマシン設定のメニューを実行するようにして動作を終了し、これ以外のときにはそのまま動作を終了する。

【００８６】なお、ステップａ９０のエラー表示は必要に応じて行えばよく、ステップａ８４で指紋データが一致しないときには直ちに動作を終了しても構わない。

【００８７】図１８は、情報処理装置３１の第９動作を示すフローチャートである。このフローチャートは図１５のフローチャートのステップａ８７～８９を削除してステップａ９１～ａ９３を追加したものであり、同じステップの説明は省略する。ステップａ８６で、指紋入力がどの領域Ｆ～Ｊ内になされたかを判断する。領域Ｆのときにはステップａ９１に、領域ＧまたはＩのときにはステップａ９２に、領域ＨまたはＪのときにはステップａ９３にそれぞれ進み、読出され格納された権限データのレベルであって、各領域Ｆ～Ｊで指定される権限レベルでネットワーク接続のメニューを実行するようにして動作を終了し、これ以外のときにはそのまま動作を終了する。

【００８８】図１９は、情報処理装置３１の第１０動作を示すフローチャートである。ステップａ１０１では、表示・指紋読取部３４の表示・データ読取画面５９に図２０に示されるような報告書８３を有する画面８１が設定され表示される。報告書８３には捺印欄８２が設定されている。なお、該捺印欄８２は指紋入力領域でもある。また、記憶部３８に記憶された指紋データが読出され記憶部４０に格納される。

【００８９】次のステップａ１０２では、報告書８３への指の接触による指紋の入力操作があったか否かを中央処理部３２が判断する。報告書８３に指が接触されて、指紋の入力操作があったと判断すると、次のステップａ１０３に進む。ここで、指の接触は画面８１の全体であっても構わない。

【００９０】ステップａ１０３では、指紋データセンシング制御部３３は表示・指紋読取部３４から指紋データと指が接触された位置の座標データとを読出し、記憶部５８に一時記憶し、記憶部４０に転送する。次のステップａ１０４では、指紋の入力が捺印欄８２内へなされたか否かを判断する。捺印欄８２内であったときにはステップａ１０５に進み、それ以外であったときにはステップａ１１１に進んでエラー表示を行って動作を終了する。

【００９１】ステップａ１０５では、指紋データを照合し認証して、一致しているか否かを判断する。一致しているときにはステップａ１０６に進み、一致していないときにはステップａ１１１に進んで、エラー表示を行って動作を終了する。

【００９２】ステップａ１０６では、関連データに基づいて、一致した指紋データが報告書の捺印権限所有者か否かを判断する。判断結果が肯定であったときにはステップａ１０７に進み、否定であったときにはステップａ１１０に進んで承認権限がない旨の表示を行って動作を終了する。

【００９３】ステップａ１０７では、報告書に次の捺印者が設定されているか否かを判断する。設定されているときにはステップａ１０８に進み、設定されていないときにはステップａ１０９に進む。ステップａ１０８では、報告書に指紋入力者の承認印を付加し、承認印が付加された報告書を次の捺印者に回覧する。すなわち、ネットワークを介して次の捺印者にデータ送信する。そして動作を終了する。ステップａ１０９では、報告書に指紋入力者の承認印を付加し、承認印が付加された報告書を報告書ファイルに設定されている保管場所に保管して、動作を終了する。

【００９４】なお、ステップａ１１０の表示やステップａ１１１のエラー表示は必要に応じて行えばよく、ステップａ１０５で指紋データが一致しないときやステップａ１０６で判断が否定であったときには直ちに動作を終了しても構わない。

【００９５】図２１は、情報処理装置３１の第１１動作を示すフローチャートである。ステップａ１２１では、表示・指紋読取部３４の表示・データ読取画面５９に図２２に示されるような決済承認願８６を有する画面８４が設定され表示される。決済承認願８６には捺印欄８５が設定されている。なお、該捺印欄８５は指紋入力領域でもある。また、記憶部３８に記憶された指紋データが読出され記憶部４０に格納される。

【００９６】次のステップａ１２２では、決済承認願８６への指の接触による指紋の入力操作があったか否かを中央処理部３２が判断する。決済承認願８６に指が接触されて、指紋の入力操作があったと判断すると、次のステップａ１２３に進む。ここで、指の接触は画面８４の全体であっても構わない。

【００９７】ステップａ１２３では、指紋データセンシング制御部３３は表示・指紋読取部３４から指紋データと指が接触された位置の座標データとを読出し、記憶部５８に一時記憶し、記憶部４０に転送する。次のステップａ１２４では、指紋の入力が捺印欄８５内へなされたか否かを判断する。捺印欄８５内であったときにはステップａ１２５に進み、それ以外であったときにはステップａ１３１に進んでエラー表示を行って動作を終了する。

【００９８】ステップａ１２５では、指紋データを照合し認証して、一致しているか否かを判断する。一致しているときにはステップａ１２６に進み、一致していないときにはステップａ１３１に進んで、エラー表示を行って動作を終了する。

【００９９】ステップａ１２６では、関連データに基づいて、一致した指紋データが決済承認願の捺印権限所有者か否かを判断する。判断結果が肯定であったときにはステップａ１２７に進み、否定であったときにはステップａ１３０に進んで承認権限がない旨の表示を行って動作を終了する。

【０１００】ステップａ１２７では、決済承認願の合計金額が承認者の決裁権限内か否かを判断する。権限内であるときにはステップａ１２９に進み、権限内でないときにはステップａ１２８に進む。ステップａ１２８では、決済承認願に指紋入力者の承認印を付加し、承認印が付加された決済承認願次の承認者に回覧する。すなわち、ネットワークを介して次の承認者にデータ送信する。そして動作を終了する。ステップａ１２９では、決済承認願に指紋入力者の承認印を付加し、承認印が付加された決済承認願を決済承認願ファイルに設定されている保管場所に保管しさらに注文書の発行処理を行って、動作を終了する。

【０１０１】なお、ステップａ１３０の表示やステップａ１３１のエラー表示は必要に応じて行えばよく、ステップａ１２５で指紋データが一致しないときやステップａ１２６で判断が否定であったときには直ちに動作を終了しても構わない。

【０１０２】図２３は、本発明の実施の他の形態である情報処理装置５７のブロック図である。情報処理装置５７は前記情報処理装置３１とほぼ同様にして構成されるが、座標指定手段としてマウス５２を有し、該マウス５２に指紋読取部の読取面５０を形成したことを特徴とする。前記装置３１と同様の構成要素には同じ参照符号を付して示す。

【０１０３】指紋認証機能を備える情報処理装置５７の中央処理部３２には、指紋読取動作を制御する指紋データセンシング制御部４９、表示部５１の表示動作を制御する表示制御部３６、マウス５２の動作を制御するポインタ制御部５５、マウスによって指定される表示面上の指紋読取りに関連した座標位置を検出する指紋読取り位置検出部５６、キー入力部３７、記憶部３８、入出力部３９および記憶部４０が接続され、装置全体の動作を統括的に制御する。

【０１０４】表示部５１は、たとえば液晶表示装置で実現され、直交座標が設定された表示面を有する。指紋読取部は、たとえば公知の技術によって実現され、指が接触される指紋読取面５０を有する。該指紋読取面５０はマウス５２の表面に形成され、たとえばマウス５２が有する左右ボタン５３，５４のうちの一方ボタン、ここでは左ボタン５３に形成される。中央処理部３２は、指紋読取り位置検出部５６によって検出され取得された座標データに基づいて、前記情報処理装置３１と同様に情報処理装置５７の動作を制御し、また取得された指紋データに基づいて前記装置３１と同様に装置５７の動作を制

御する。

【０１０５】

【発明の効果】以上のように本発明によれば、指紋認証機能を備える情報処理装置において、指紋認証時における表示面上の指紋読取りに関連した座標指定という簡単な操作によって、座標に基づく情報処理装置の動作制御が可能となる。

【０１０６】また本発明によれば、表示面と指紋読取面とを同一としたので、指紋入力と座標指定とを同一の操作で行うことができ、高い操作性が得られる。

【０１０７】また本発明によれば、座標指定手段に指紋読取面を形成したので、座標指定と指紋入力とを同一の操作で行うことができ、高い操作性が得られる。

【０１０８】また本発明によれば、特定座標が指定されたときのみに指紋認証を行うようにしたので、高いセキュリティ性を得ることができる。

【０１０９】また本発明によれば、指紋認証機能を備える情報処理装置において、指紋認証時における表示面上の指紋読取りに関連した座標が指定され、指定された座標から暗証番号が取得される。取得された暗証番号は認証され、暗証番号の認証結果に基づく情報処理装置の動作制御が可能となる。このように、指紋認証時における暗証番号入力のための座標指定という簡単な操作によって情報処理装置の動作を制御することができる。

【０１１０】また本発明によれば、暗証番号が一致していたときのみに指紋認証を行うようにしたので、高いセキュリティ性を得ることができる。

【０１１１】また本発明によれば、指紋が一致していたときに、情報処理装置の電源の動作を制御するようにしたので、高いセキュリティ性および操作性を得ることができ、また消費電力の低減を図ることができる。

【０１１２】また本発明によれば、指紋が一致していたときに、ユーザ毎に予め設定された動作条件の中から一致した指紋のユーザに対応する動作条件を読出して設定するようにしたので、ユーザに適した操作環境や利用機能を設定することができ、高い操作性が得られる。

【０１１３】また本発明によれば、指紋認証機能において各指の指紋認証を可能としたので、各指の指紋認証結果に基づく情報処理装置の細かな動作制御が可能となる。

【０１１４】また本発明によれば、各指の指紋認証結果に基づいて、ユーザの各指毎に予め登録されたコマンドの中から一致した指紋のユーザの各指に対応するコマンドを読出して実行するようにしたので、高いセキュリティ性および操作性を得ることができ、また各指毎の細かな動作制御が可能となる。

【０１１５】また本発明によれば、指紋認証機能を備える情報処理装置において、上述したようにして座標が指定され、このときアイコン指定の判定結果および指紋認証結果に基づく情報処理装置の動作制御が可能であり、アイコンが指定されかつ指紋が一致したとき、指定されたアイコンに対応するアプリケーションの一致した指紋のユーザのデータのみを読出して表示させ、このようにして簡単な操作によって情報処理装置の動作を制御することができる。

【０１１６】また本発明によれば、アイコンが指定されかつ指紋が一致したとき、ユーザ毎に予め設定されたアプリケーションの中の一致した指紋のユーザに対応するアプリケーションを起動し、このようにして簡単な操作によって情報処理装置の動作を制御することができる。

【０１１７】また本発明によれば、アイコンが指定されかつ指紋が一致したとき、ファイルの中の指定されたアイコンに対応するファイルの一致した指紋のユーザのファイルのみを開き、このようにして簡単な操作によって情報処理装置の動作を制御することができる。

【０１１８】また本発明によれば、指紋認証機能を備える情報処理装置において、上述したようにして座標が指定され、このときメニュー実行レベル領域指定の判定結果および指紋認証結果に基づく情報処理装置の動作制御が可能であり、メニュー実行レベル領域が指定されかつ指紋が一致したとき、ユーザ毎に予め設定された実行レベルの中の一致した指紋のユーザに対応する実行レベルであって、指定されたメニュー実行レベル領域の実行レベルでメニューを実行し、このようにして簡単な操作によって情報処理装置の動作を制御することができる。

【０１１９】また本発明によれば、捺印欄を有する書類に対して捺印欄内の座標が指定されたとき、承認印が付加され、該書類が通信手段によって通信され、このようにして報告書などの書類を次の人に転送して回覧することができる。

【０１２０】また本発明によれば、捺印欄を有する書類に対して捺印欄内の座標が指定されたとき、承認印が付加され、該書類には付帯手段がなされ、このようにして決済承認類などの書類に対して注文書の発行処理を行うことができる。

【図面の簡単な説明】

【図１】本発明の実施の一形態である情報処理装置３１のブロック図である。

【図２】表示・指紋読取部３４の表示・データ読取画面５９を示す図である。

【図３】記憶部３８のユーザ登録データを示す図である。

【図４】情報処理装置を３１の第１動作を示すフローチャートである。

【図５】情報処理装置を３１の第２動作を示すフローチャートである。

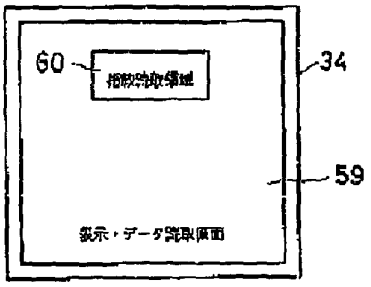
【図６】情報処理装置３１の第３動作を示すフローチャートである。

【図７】暗証番号の入力を促す画面７１を示す図である。

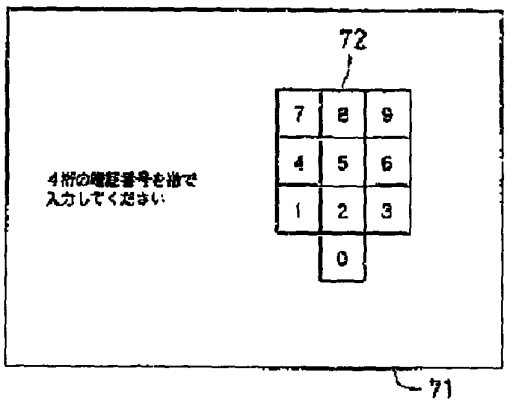
【図８】情報処理装置３１の第４動作を示すフローチャートである。
【図９】指紋の入力を促す画面７３を示す図である。
【図１０】情報処理装置３１の第５動作を示すフローチャートである。
【図１１】指紋の入力を促す画面７５を示す図である。
【図１２】情報処理装置３１の第６動作を示すフローチャートである。
【図１３】情報処理装置３１の第７動作を示すフローチャートである。
【図１４】アイコンの指定を促す画面７７を示す図である。
【図１５】情報処理装置３１の第８動作を示すフローチャートである。
【図１６】メニューの指定を促す画面７９を示す図である。
【図１７】前記画面７９のメニュー指定領域８０ａ，８０ｂの複数の領域Ａ～Ｊを示す図である。
【図１８】情報処理装置３１の第９動作を示すフローチャートである。
【図１９】情報処理装置３１の第１０動作を示すフローチャートである。
【図２０】報告書８３を有する画面８１を示す図である。
【図２１】情報処理装置３１の第１１動作を示すフローチャートである。
【図２２】決済承認願８６を有する画面８４を示す図である。
【図２３】本発明の実施の他の形態である情報処理装置５７のブロック図である。
【図２４】従来技術の情報処理装置１のブロック図である。
【図２５】情報処理装置１の指紋読取部４と表示部７とを示す図である。

【符号の説明】
３１，５７　情報処理装置
３２　中央処理部
３３，４９　指紋データセンシング制御部
３４　表示・指紋読取部
３５　指紋センシングエリア設定部
３６　表示制御部
３８，４０　記憶部
３９　入出力部
４１　プログラム・ワークメモリ
４２　指紋認証部
４３　特徴抽出部
４４　照合部
４５　指紋・関連データ読出し・格納部
４６　読出部
４７　格納部
４８　アプリケーションプログラム格納部
５０　指紋読取面
５１　表示部
５２　マウス
５３　左ボタン
５４　右ボタン
５５　ポインタ制御部
５６　指紋読取位置検出部
５８　座標位置・指紋データ記憶部
５９　表示・データ読取画面
６０　指紋読取領域

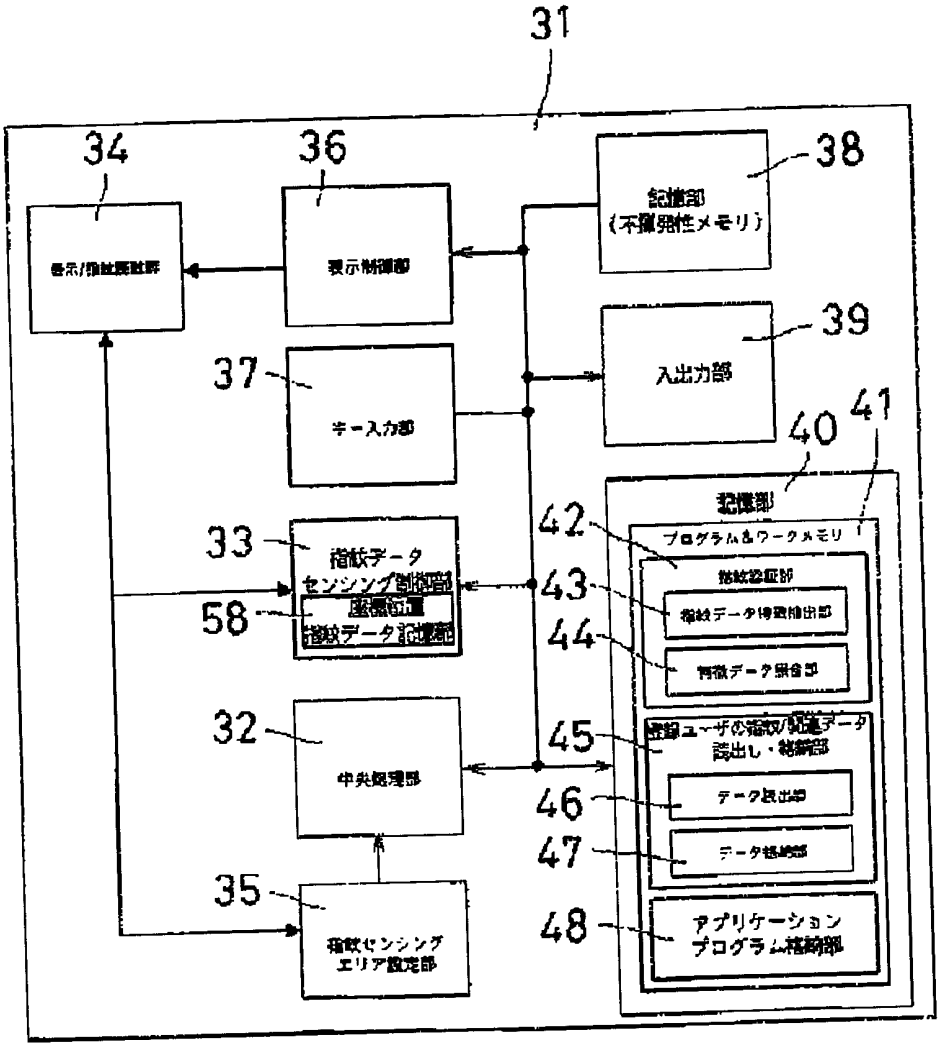
【図２】



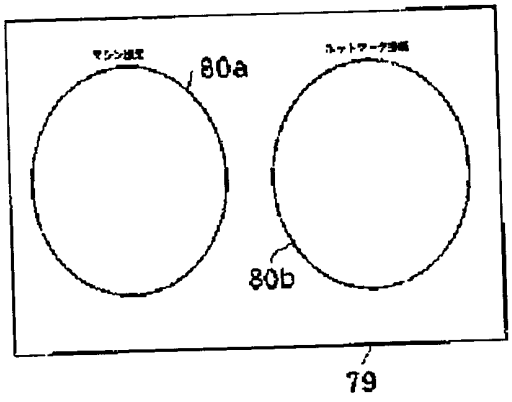
【図７】



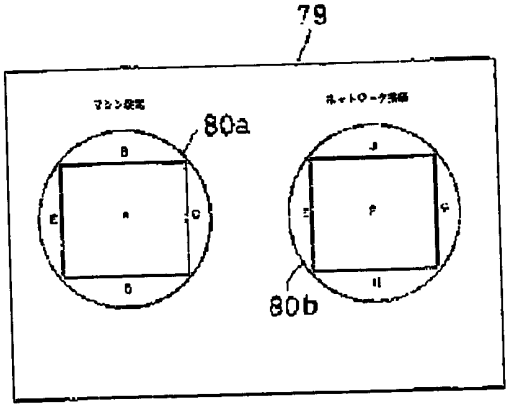
【図1】


31
34
36
38
表示/指紋画像部
表示制御部
記憶部
(不揮発性メモリ)
39
入出力部
37
キー入力部
40
41
記憶部
42
プログラム&ワークメモリ
33
指紋データ
センシング制御部
43
指紋認証部
指紋データ特徴抽出部
58
44
指紋データ照合部
32
中央処理部
45
登録ユーザの指紋/特徴データ
読出し・格納部
46
データ読出部
47
データ格納部
35
指紋センシング
エリア設定部
48
アプリケーション
プログラム格納部

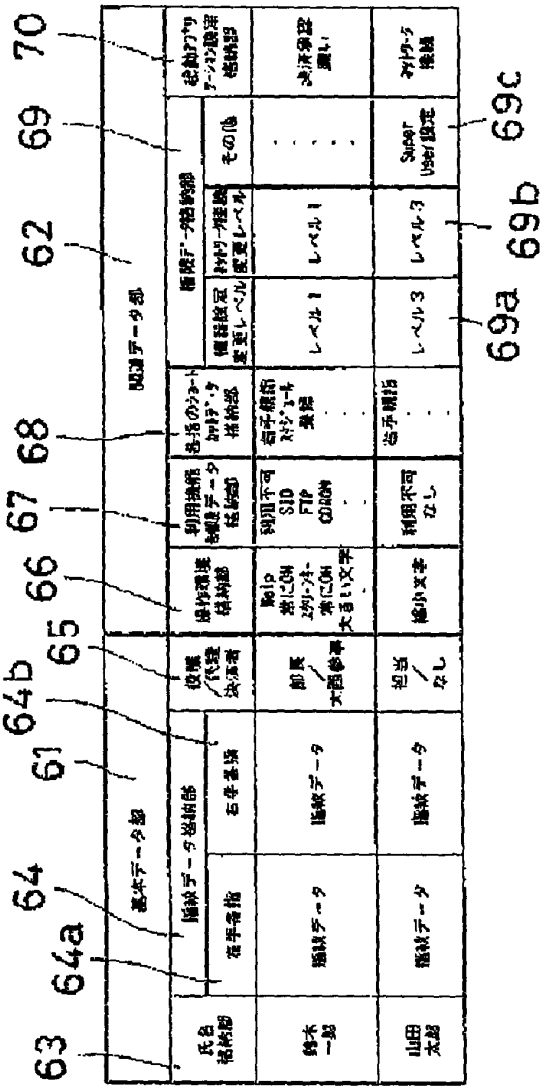
【図16】


80a
80b
79

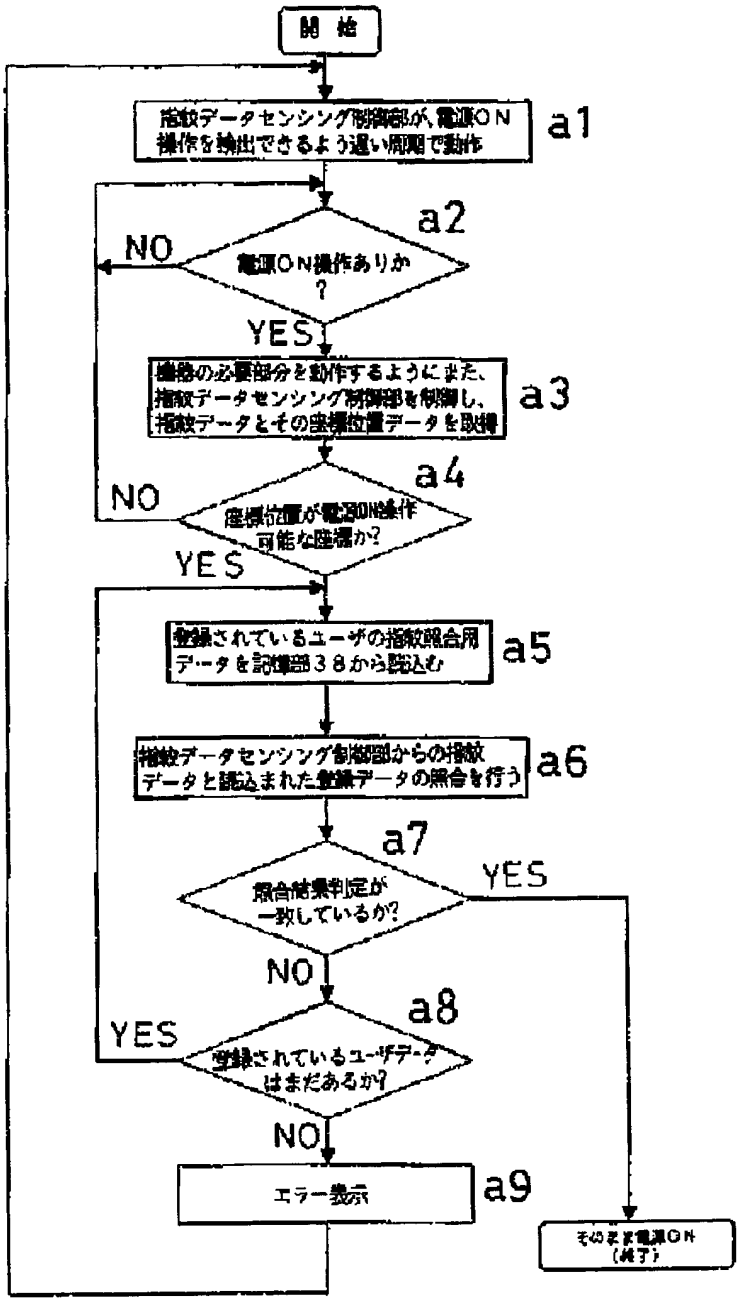
【図17】


79
80a
80b

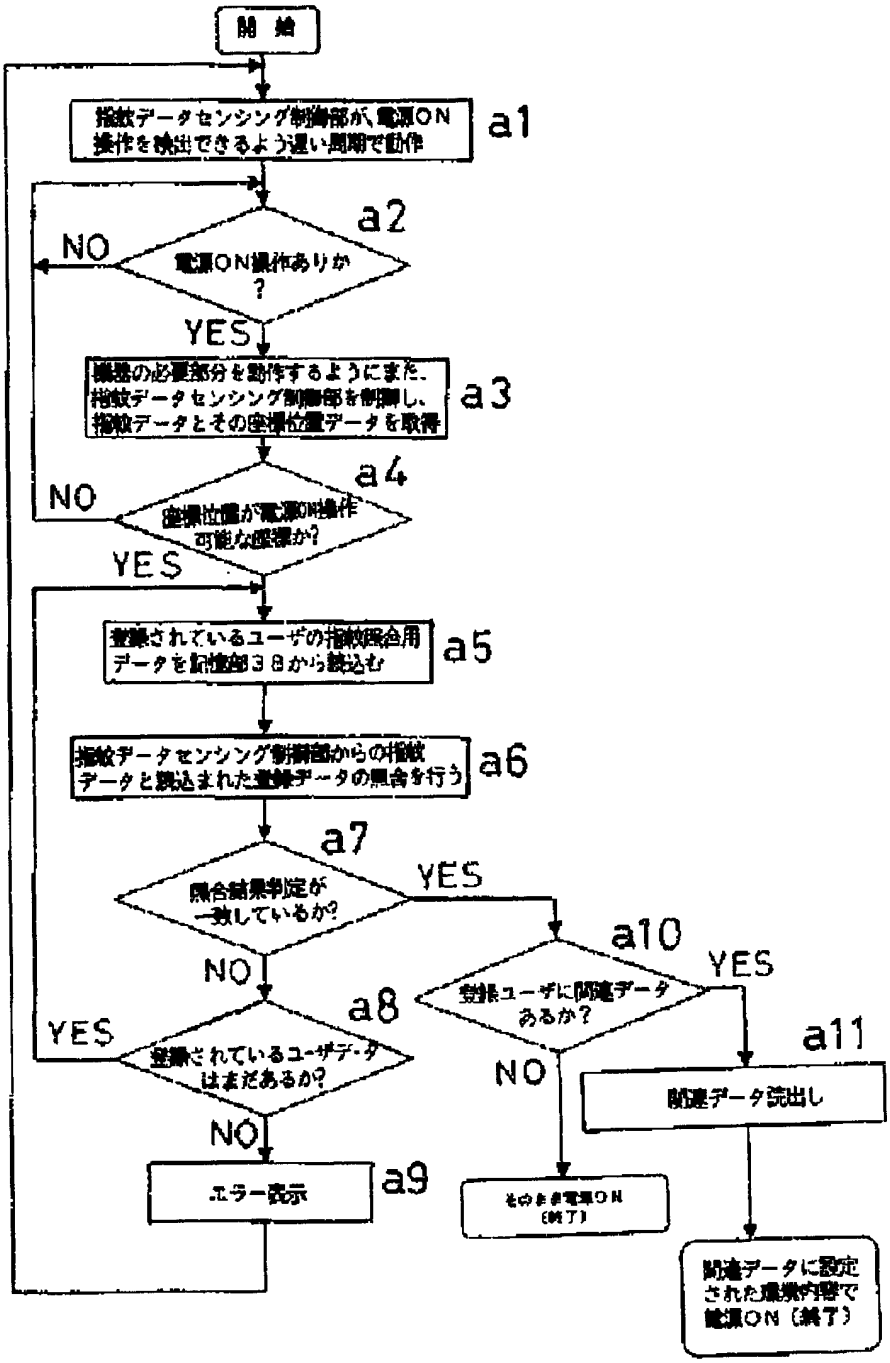
【図3】


63
64
64a
61
64b
65
66
67
68
62
69
69a
69b
69c
70
基本データ部
関連データ部
氏名格納部
指紋データ格納部
右手人指
右手他指
役職/代理決裁者
操作環境格納部
利用抑制制御データ格納部
操作のショートカットデータ格納部
権限データ格納部
権限設定変更レベル
ネットワーク権限変更レベル
その他
追加アプリケーション設定格納部
鈴木一郎
指紋データ
指紋データ
部長/大臣参事
Help 表示ON/OFF 常にON 大きい文字
利用不可 SIO FTP CORON
右手人指 パターン1-4 登録
レベル1
レベル1
未使用登録無し
山田太郎
指紋データ
指紋データ
担当/なし
縮小文字
利用不可 なし
右手親指
レベル3
レベル3
Super User 設定
オプション機能

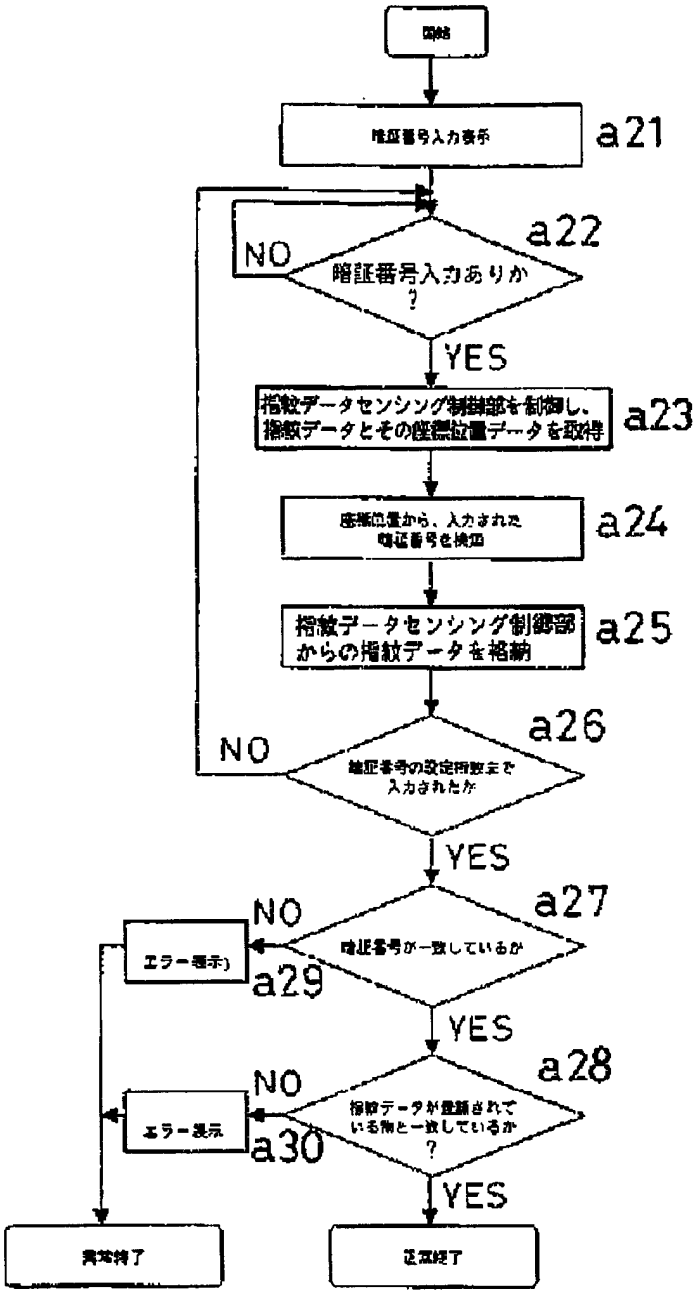
【図４】


開始
指紋データセンシング制御部が、電源ON操作を検出できるよう遅い周期で動作
a1
a2
NO
電源ON操作ありか？
YES
機器の必要部分を動作するようにまた、指紋データセンシング制御部を制御し、指紋データとその座標位置データを取得
a3
a4
NO
座標位置が電源ON操作可能な座標か？
YES
登録されているユーザの指紋照合用データを記憶部３８から読込む
a5
指紋データセンシング制御部からの指紋データと読込まれた登録データの照合を行う
a6
a7
照合結果判定が一致しているか？
YES
NO
a8
YES
登録されているユーザデータはまだあるか？
NO
エラー表示
a9
その後電源ON（終了）

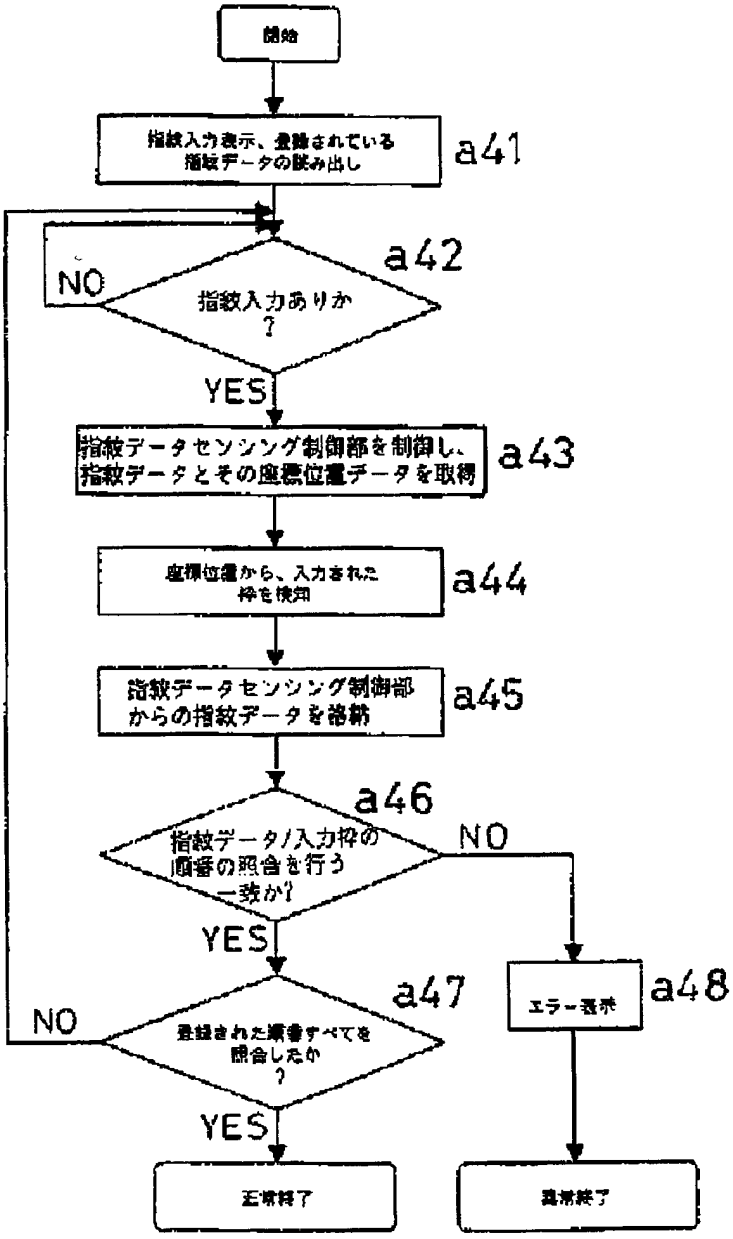
【図5】


開始
指紋データセンシング制御部が、電源ON操作を検出できるよう遅い周期で動作
a1
a2
NO
電源ON操作ありか？
YES
機器の必要部分を動作するようにまた、指紋データセンシング制御部を制御し、指紋データとその座標位置データを取得
a3
a4
NO
座標位置が電源ON操作可能な座標か？
YES
登録されているユーザの指紋照合用データを記憶部38から読込む
a5
指紋データセンシング制御部からの指紋データと読込まれた登録データの照合を行う
a6
a7
照合結果判定が一致しているか？
YES
NO
a8
YES
登録されているユーザデータはまだあるか？
NO
エラー表示
a9
a10
登録ユーザに関連データあるか？
YES
NO
a11
関連データ読出し
そのまま電源ON（終了）
関連データに設定された起業内容で電源ON（終了）

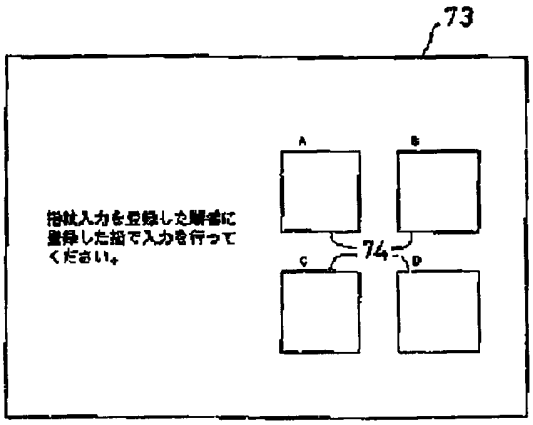
【図６】


開始
暗証番号入力表示
a21
NO
a22
暗証番号入力ありか
?
YES
指紋データセンシング制御部を制御し、指紋データとその座標位置データを取得
a23
座標位置から、入力された暗証番号を検出
a24
指紋データセンシング制御部からの指紋データを格納
a25
NO
a26
暗証番号の設定桁数全て入力されたか
YES
NO
a27
暗証番号が一致しているか
エラー表示
a29
YES
NO
a28
指紋データが登録されている物と一致しているか
?
エラー表示
a30
YES
異常終了
正常終了

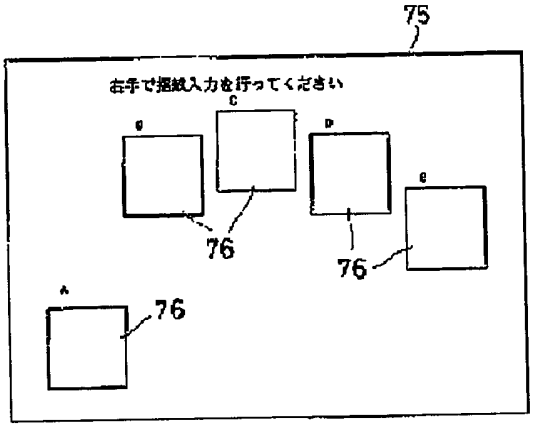
【図8】


開始
指紋入力表示、登録されている指紋データの読み出し
a41
NO
指紋入力ありか？
a42
YES
指紋データセンシング制御部を制御し、指紋データとその座標位置データを取得
a43
座標位置から、入力された枠を検知
a44
指紋データセンシング制御部からの指紋データを読取
a45
指紋データ/入力枠の順番の照合を行う一致か?
a46
NO
YES
エラー表示
a48
登録された順番すべてを照合したか？
a47
NO
YES
正常終了
異常終了

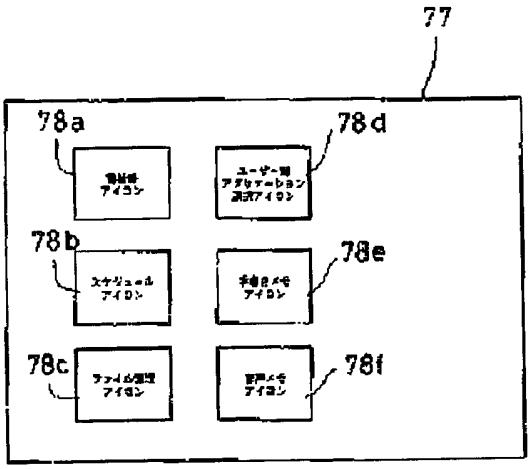
【図９】



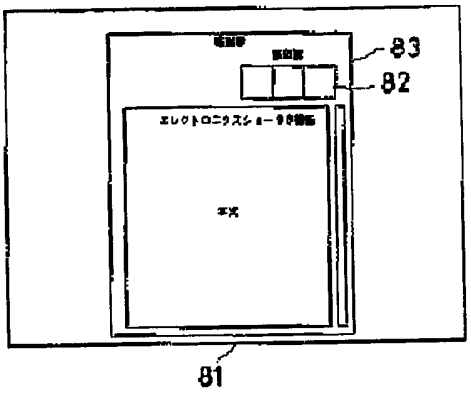
【図１１】



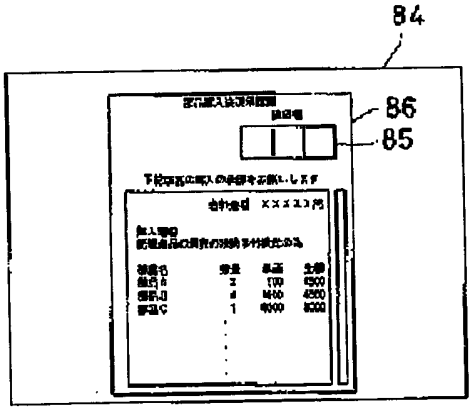
【図１４】



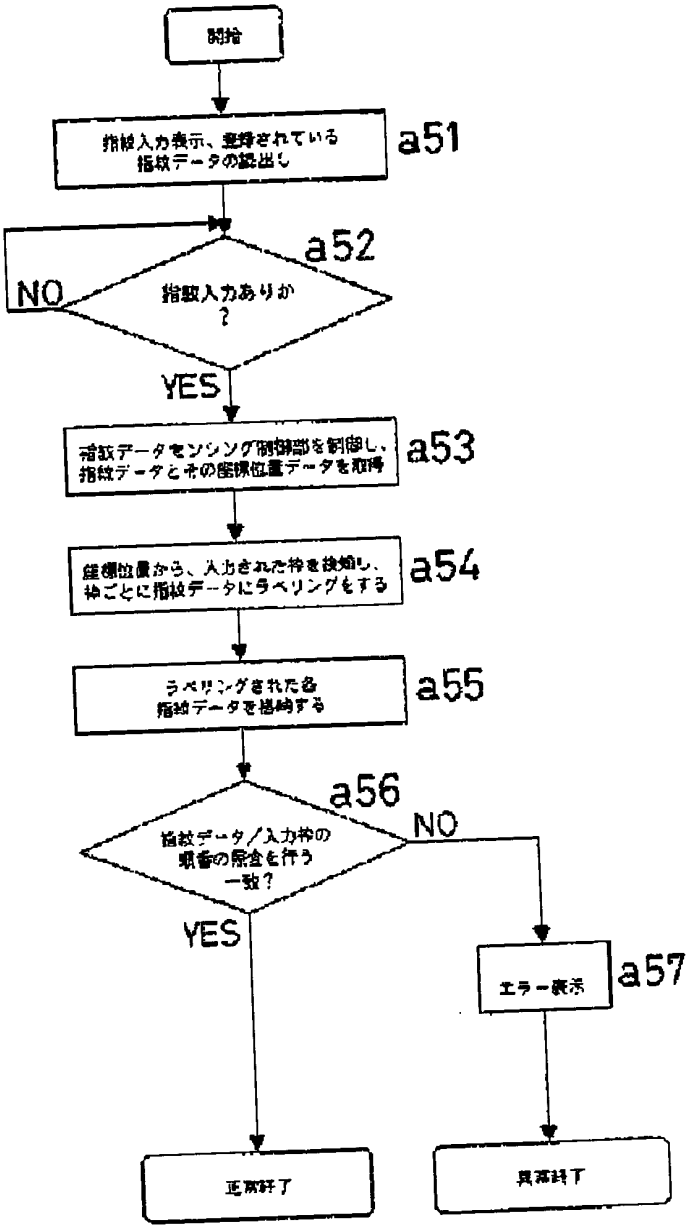
【図２０】



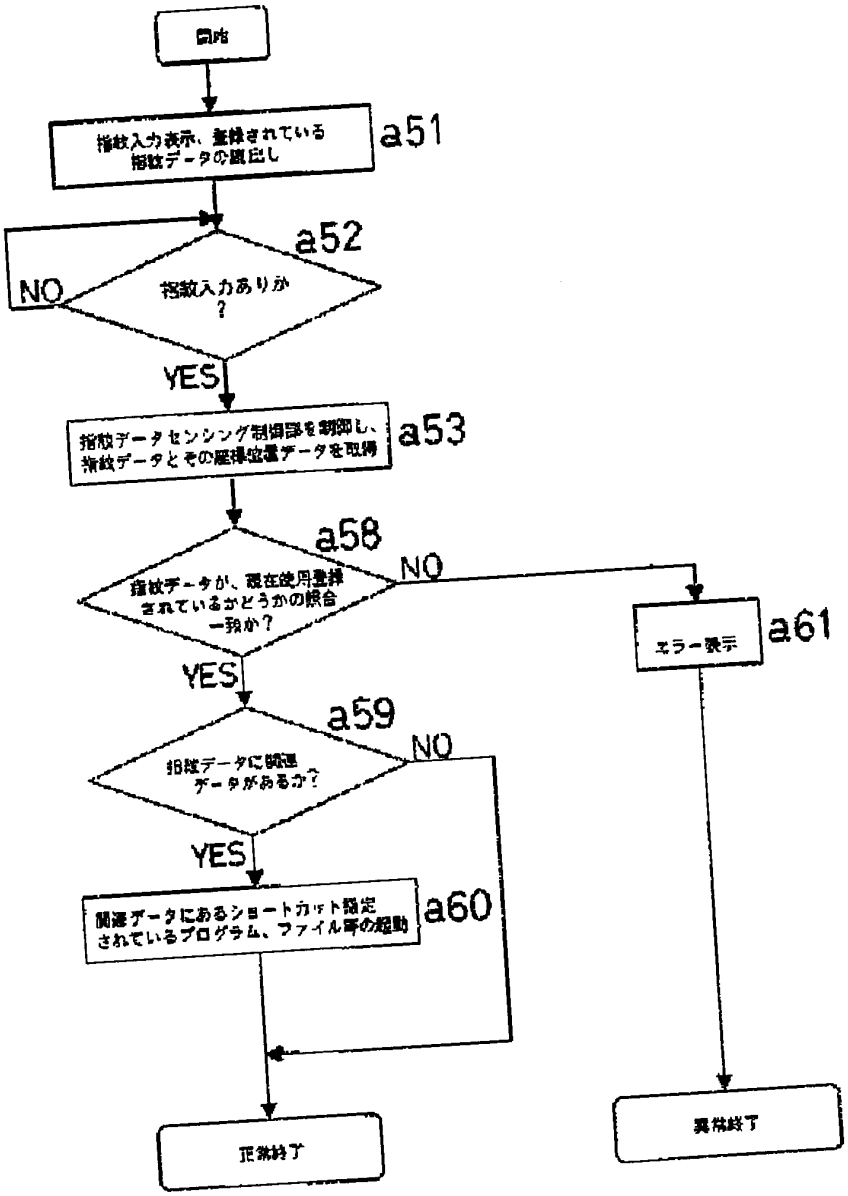
【図２２】



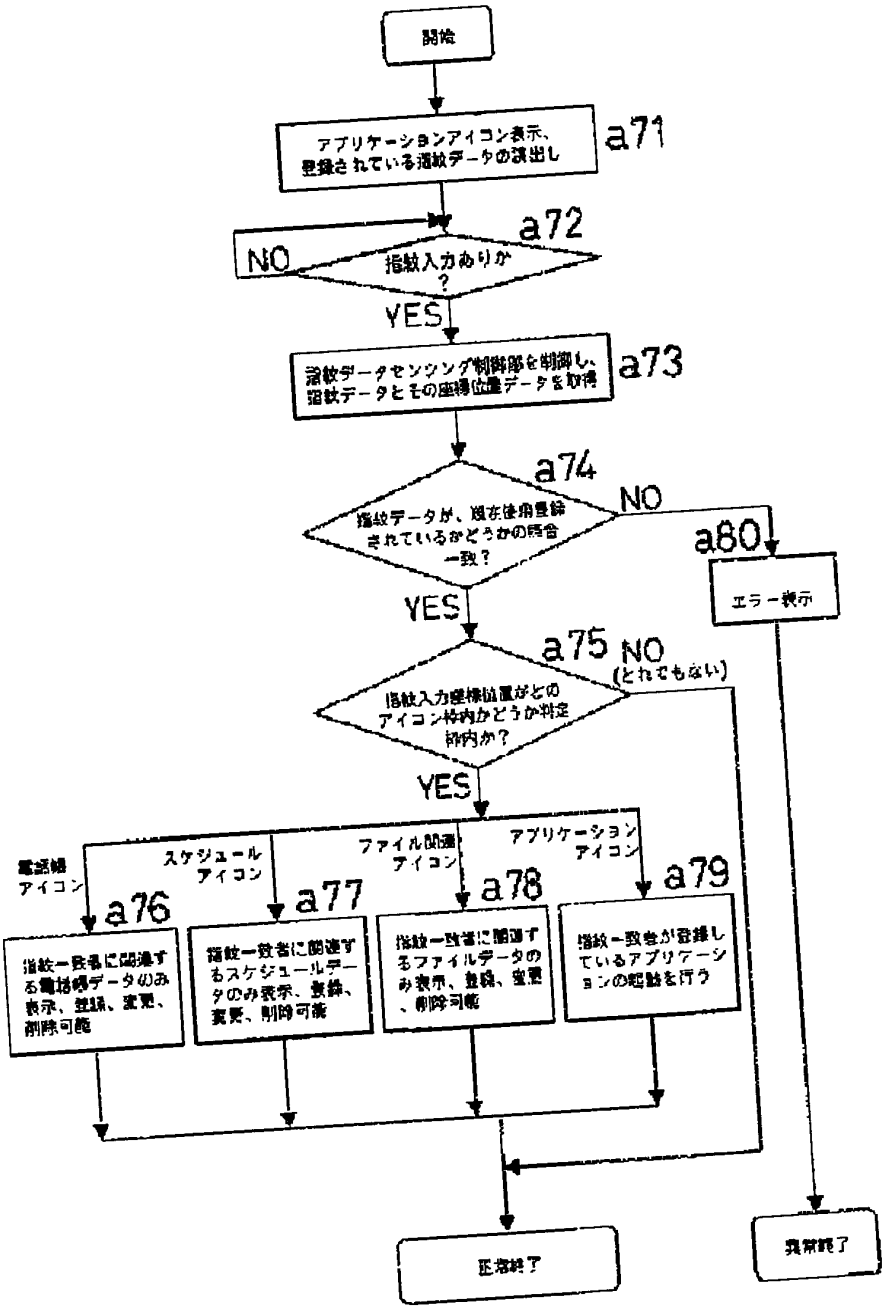
【図１０】


開始
指紋入力表示、登録されている指紋データの読出し
a51
a52
NO
指紋入力ありか？
YES
指紋データセンシング制御部を制御し、指紋データとその座標位置データを取得
a53
座標位置から、入力された枠を検知し、枠ごとに指紋データにラベリングをする
a54
ラベリングされた各指紋データを格納する
a55
a56
指紋データ／入力枠の順番の照合を行う一致？
NO
YES
エラー表示
a57
正常終了
異常終了

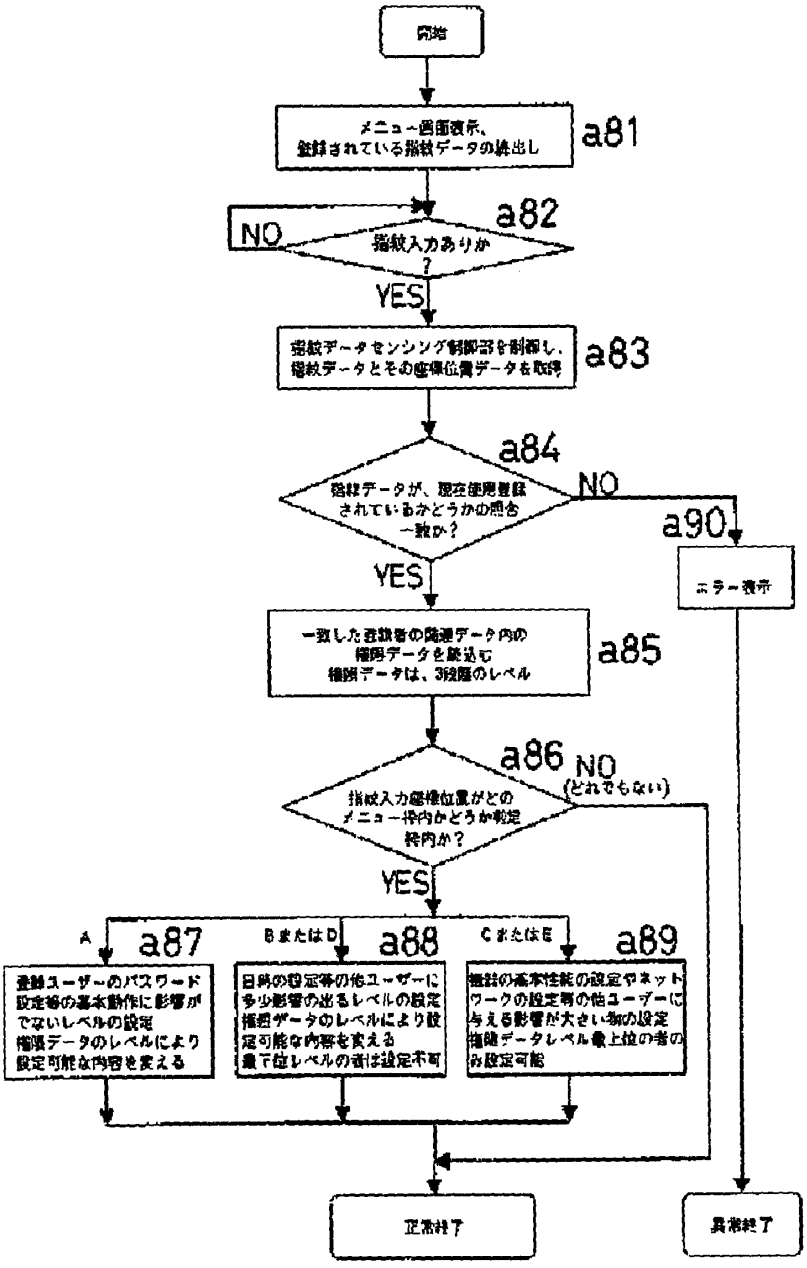
【図12】


開始
指紋入力表示、登録されている指紋データの読出し
a51
a52
NO
指紋入力ありか？
YES
指紋データセンシング制御部を制御し、指紋データとその座標位置データを取得
a53
a58
指紋データが、現在使用登録されているかどうかの照合一致か？
NO
エラー表示
a61
YES
a59
NO
指紋データに関連データがあるか？
YES
関連データにあるショートカット指定されているプログラム、ファイル等の起動
a60
正常終了
異常終了

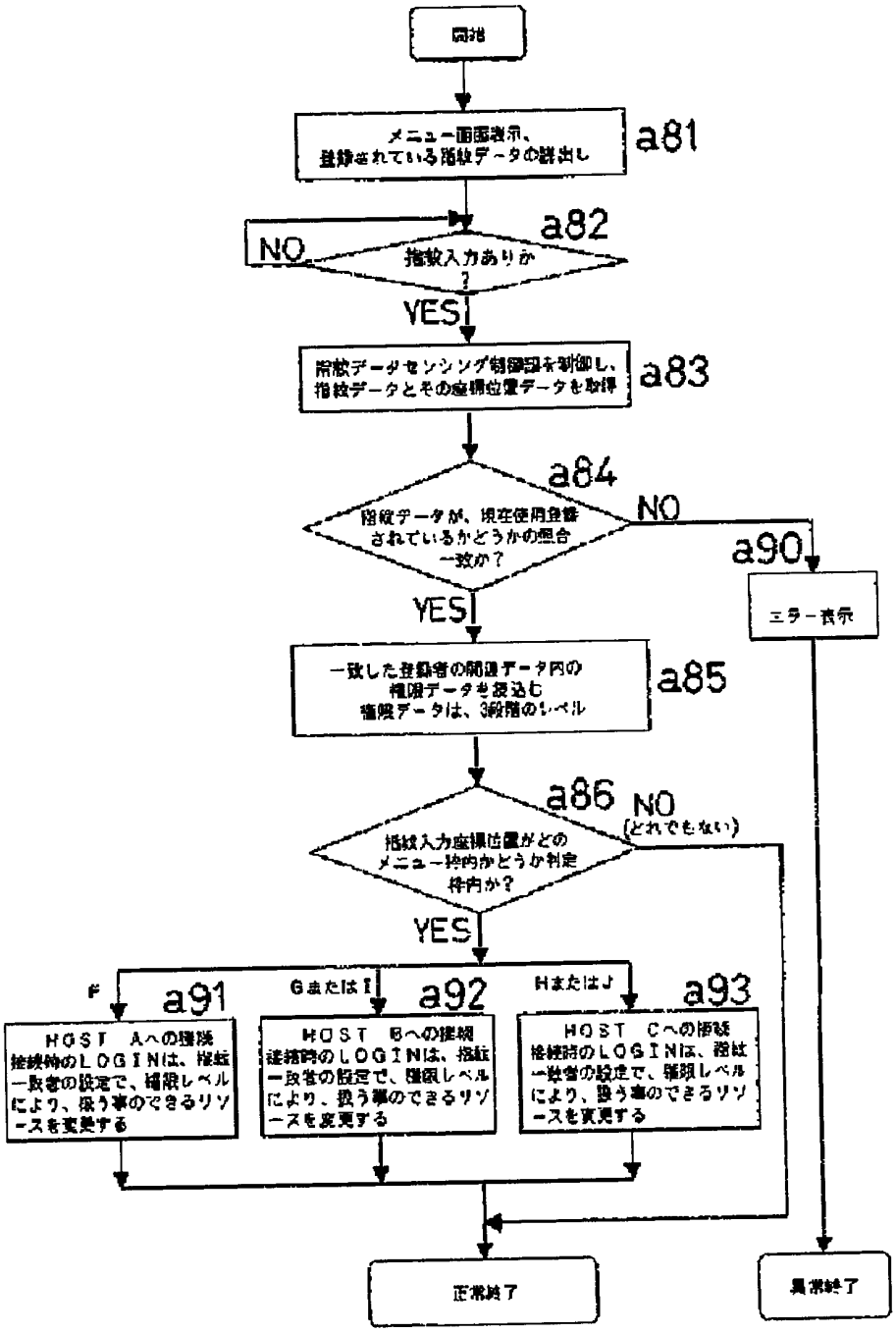
【図13】


開始
アプリケーションアイコン表示、登録されている指紋データの読出し
a71
NO
a72
指紋入力ありか？
YES
指紋データセンシング制御部を制御し、指紋データとその座標位置データを取得
a73
a74
指紋データが、現在使用登録されているかどうかの照合一致？
NO
a80
エラー表示
YES
a75
NO
(どれでもない)
指紋入力座標位置がどのアイコン枠内かどうか判定
枠内か？
YES
電話帳アイコン
スケジュールアイコン
ファイル関連アイコン
アプリケーションアイコン
a76
指紋一致者に関連する電話帳データのみ表示、登録、変更、削除可能
a77
指紋一致者に関連するスケジュールデータのみ表示、登録、変更、削除可能
a78
指紋一致者に関連するファイルデータのみ表示、登録、変更、削除可能
a79
指紋一致者が登録しているアプリケーションの起動を行う
正常終了
異常終了

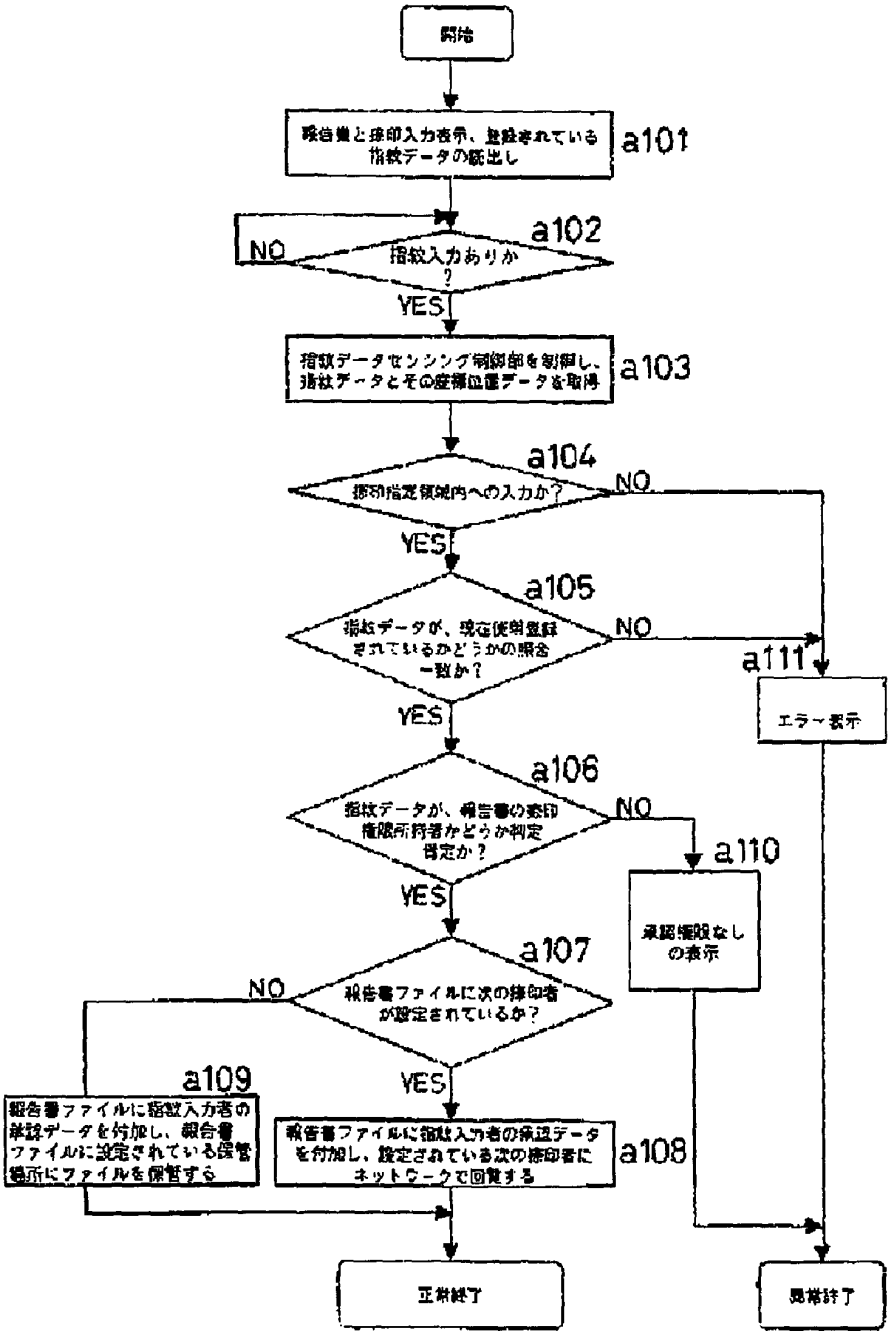
【図15】


開始
メニュー画面表示、
登録されている指紋データの読出し
a81
NO
a82
指紋入力ありか
?
YES
指紋データセンシング制御部を制御し、
指紋データとその座標位置データを取得
a83
a84
指紋データが、現在使用者登録
されているかどうかの照合
一致か?
NO
a90
エラー表示
YES
一致した登録者の関連データ内の
権限データを読込む
権限データは、3段階のレベル
a85
a86
NO
(どれでもない)
指紋入力座標位置がどの
メニュー枠内かどうか判定
枠内か?
YES
A
a87
B または D
a88
C または E
a89
登録ユーザーのパスワード
設定等の基本動作に影響が
でないレベルの設定
権限データのレベルにより
設定可能な内容を変える
日時の設定等の他ユーザーに
多少影響の出るレベルの設定
権限データのレベルにより設
定可能な内容を変える
最下位レベルの者は設定不可
機器の基本性能の設定やネット
ワークの設定等の他ユーザーに
与える影響が大きい物の設定
権限データレベル最上位の者の
み設定可能
正常終了
異常終了

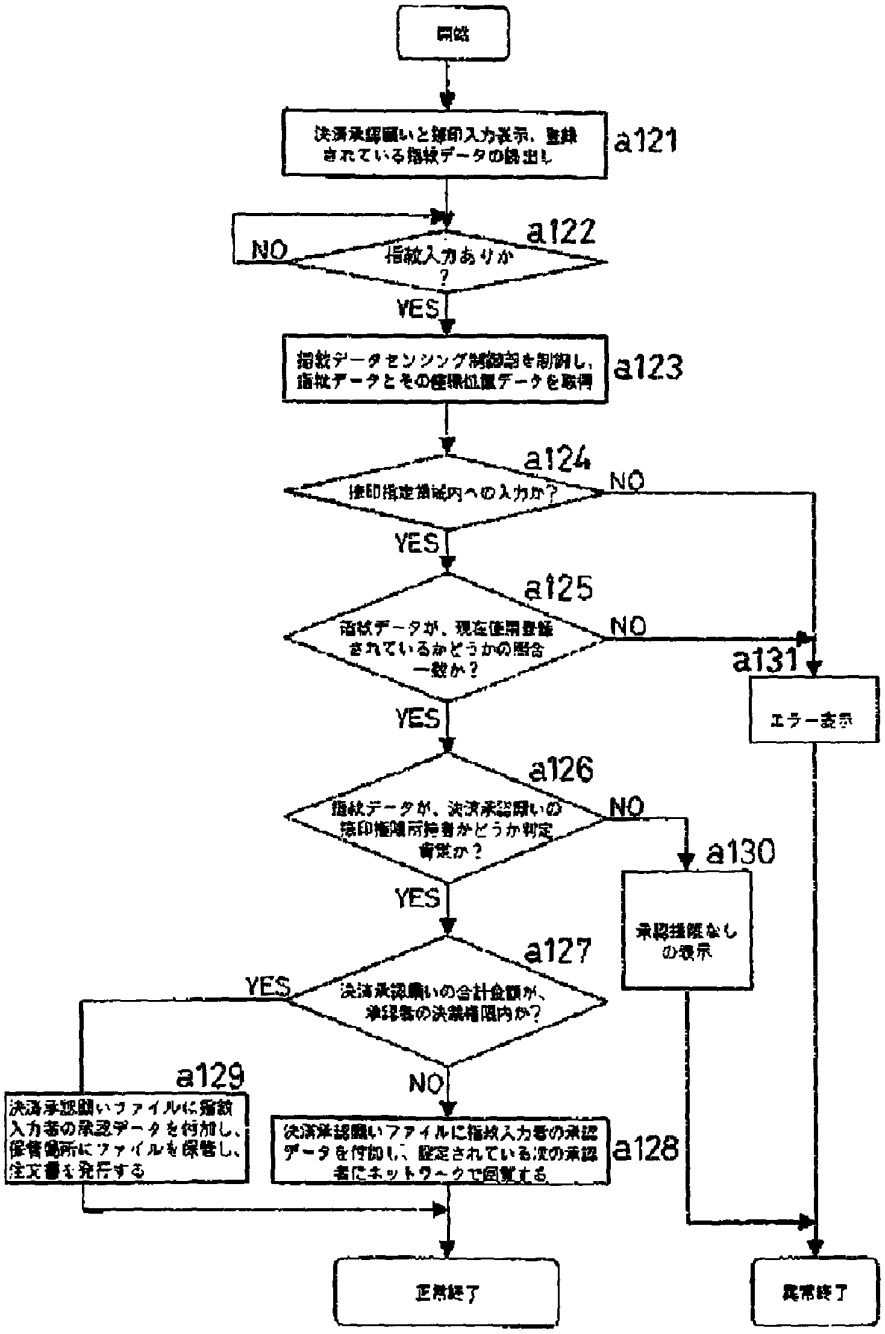
【図１８】


開始
メニュー画面表示、
登録されている指紋データの読出し
a81
a82
NO
指紋入力ありか
？
YES
指紋データセンシング制御部を制御し、
指紋データとその座標位置データを取得
a83
a84
指紋データが、現在使用登録
されているかどうかの照合
一致か？
NO
a90
エラー表示
YES
一致した登録者の関連データ内の
権限データを読込む
権限データは、3段階のレベル
a85
a86
NO
(どれでもない)
指紋入力座標位置がどの
メニュー枠内かどうか判定
枠内か？
YES
F
a91
G またはI
a92
HまたはJ
a93
HOST Aへの接続
接続時のLOGINは、指紋
一致者の設定で、権限レベル
により、扱う事のできるリソ
ースを変更する
HOST Bへの接続
接続時のLOGINは、指紋
一致者の設定で、権限レベル
により、扱う事のできるリソ
ースを変更する
HOST Cへの接続
接続時のLOGINは、指紋
一致者の設定で、権限レベル
により、扱う事のできるリソ
ースを変更する
正常終了
異常終了

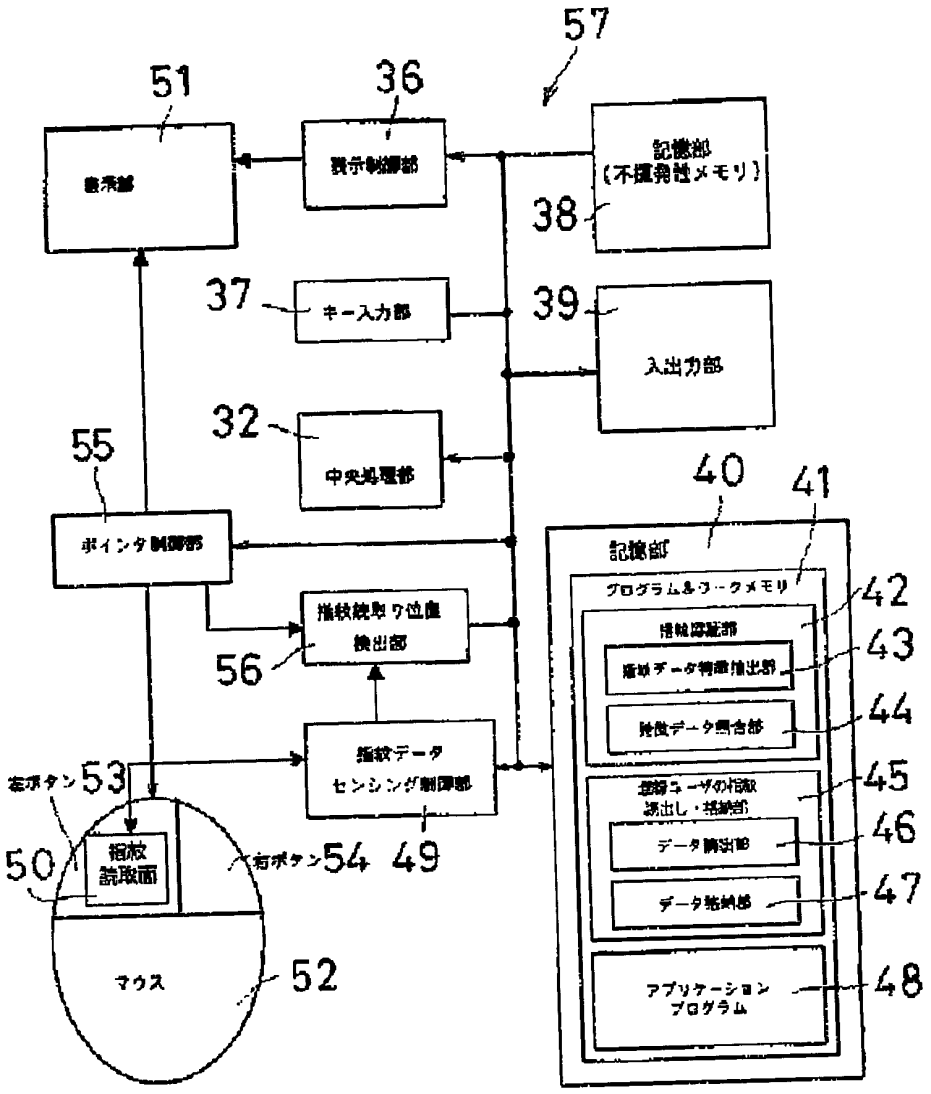
【図19】


開始
報告書と捺印入力表示、登録されている指紋データの読出し
a101
a102
NO
指紋入力あり か ?
YES
指紋データセンシング制御部を制御し、指紋データとその座標位置データを取得
a103
a104
捺印指定領域内への入力か?
NO
YES
a105
指紋データが、現在使用登録されているかどうかの照合一致か?
NO
YES
a111
エラー表示
a106
指紋データが、報告書の捺印権限所持者かどうか判定指定か?
NO
YES
a110
承認権限なしの表示
a107
報告書ファイルに次の捺印者が設定されているか?
NO
YES
a109
報告書ファイルに指紋入力者の承認データを付加し、報告書ファイルに設定されている保管場所にファイルを保管する
報告書ファイルに指紋入力者の承認データを付加し、設定されている次の捺印者にネットワークで回覧する
a108
正常終了
異常終了

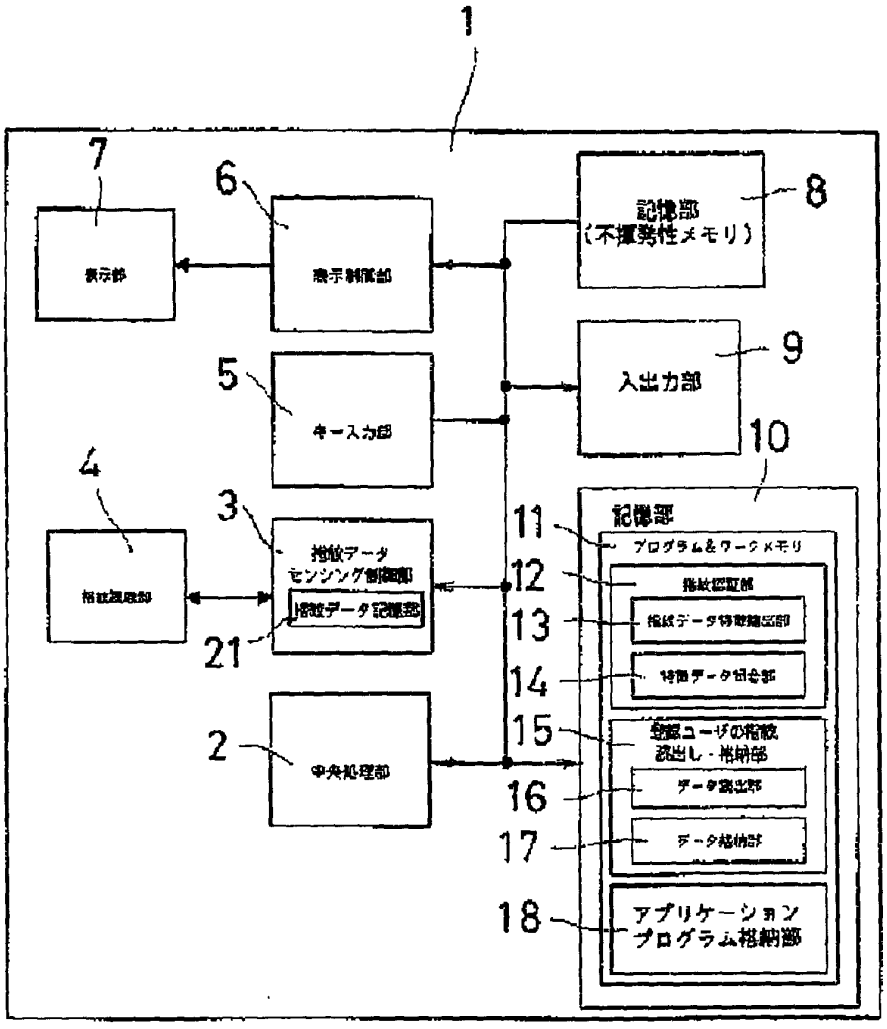
【図21】


開始
決済承認願いと捺印入力表示、登録されている指紋データの読出し
a121
NO
a122
指紋入力ありか？
YES
指紋データセンシング制御部を制御し、指紋データとその座標位置データを取得
a123
a124
捺印指定領域内への入力か？
NO
YES
a125
指紋データが、現在使用登録されているかどうかの照合一致か？
NO
YES
a131
エラー表示
a126
指紋データが、決済承認願いの捺印権限所持者かどうか判定有効か？
NO
YES
a130
承認権限なしの表示
a127
決済承認願いの合計金額が、承認者の決裁権限内か？
YES
NO
a129
決済承認願いファイルに指紋入力者の承認データを付加し、保管場所にファイルを保管し、注文書を発行する
決済承認願いファイルに指紋入力者の承認データを付加し、設定されている次の承認者にネットワークで回覧する
a128
正常終了
異常終了

【図23】

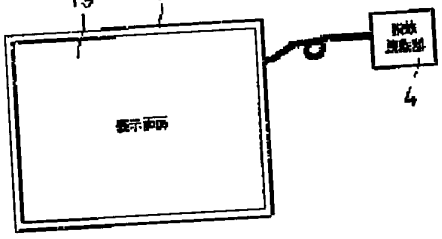

57
51
36
表示部
表示制御部
記憶部
(不揮発性メモリ)
38
37
キー入力部
39
入出力部
32
中央処理部
55
40
41
ポインタ制御部
記憶部
プログラム&ワークメモリ
42
43
44
45
46
47
48
指紋データ特徴抽出部
照合部
データ抽出部
データ格納部
アプリケーション
プログラム
指紋統計位置
検出部
56
指紋データ
センシング制御部
49
左ボタン
53
50
指紋
読取面
右ボタン
54
マウス
52

【図24】


1
7
6
8
記憶部
(不揮発性メモリ)
9
入出力部
5
キー入力部
10
4
3
11
記憶部
プログラム&ワークメモリ
12
13
14
15
16
17
18
アプリケーション
プログラム格納部
21
2
中央処理部

【図２５】

(A)



(B)